Elementary Number Theory

PMATH 340

Spring 2022 (1225)

Cameron Roopnarine* Salma Shaheen†

14th July 2022

Contents

*LaTeXer

†Instructor

1 Integers

- Natural numbers: $\mathbf{N} = \{0, 1, 2, \ldots\}$.
- Ring of integers: $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$.
- Field of fractions $\mathbf{Q} = \{a/b : a, b \in \mathbf{Z} \wedge b \neq 0\}$.
- Field of real numbers: $\mathbf{R}$.
- Field of complex numbers: $\mathbf{C} = \{a + bi : a, b \in \mathbf{R} \wedge i = \sqrt{-1}\}$.

DEFINITION 1.1: Axioms

Set of integers as integral domains:

V1 $\mathbf{Z}$ has operations $+$ (addition) and $\cdot$ (multiplication). It is closed under these operations, in that if $a, b \in \mathbf{Z}$, then $a + b \in \mathbf{Z}$ and $a \cdot b \in \mathbf{Z}$.

V2 Addition is associative: If $a, b, c \in \mathbf{Z}$, then

$$a + (b + c) = (a + b) + c.$$

V3 There is an additive identity $0 \in \mathbf{Z}$: For all $a \in \mathbf{Z}$,

$$a + 0 = 0 + a = a.$$

V4 Every element has an additive inverse: If $a \in \mathbf{Z}$, there is an element $-a \in \mathbf{Z}$ such that

$$a + (-a) = 0 \text{ and } (-a) + a = 0.$$

V5 Addition is commutative: If $a, b \in \mathbf{Z}$, then

$$a + b = b + a.$$

V6 Multiplication is associative: If $a, b, c \in \mathbf{Z}$, then

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

V7 There is a multiplicative identity $1 \in \mathbf{Z}$: For all $a \in \mathbf{Z}$,

$$a \cdot 1 = a = 1 \cdot a.$$

V8 Multiplication is commutative: If $a, b \in \mathbf{Z}$, then

$$a \cdot b = b \cdot a.$$

V9 The Distributive Laws hold: If $a, b, c \in \mathbf{Z}$, then

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

V10 There are no zero divisors: If $a, b \in \mathbf{Z}$ and $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

REMARK 1.1

(i) As usual, we will often abbreviate $m \cdot n$ to mn.

(ii) The last axiom is equivalent to the **cancellation law**. If $a, b, c \in \mathbf{Z}$, $a \neq 0$, and $ab = ac$, then $b = c$.

$$\begin{aligned} ab &= ac \\ ab - ac &= 0 \\ a(b-c) &= 0. \end{aligned}$$

Since there are no zero divisors, either $a = 0$ or $b - c = 0$. Since $a \neq 0$ by assumption, we must have $b - c = 0$, so $b = c$.

Notice that we did not divide both sides of the equation by a; we cancelled a from both sides. This shows that division and cancellation are not the "the same thing."

EXERCISE 1.1

If $n \in \mathbf{Z}$, then prove that $0 \cdot n = 0$.

Solution:

$$\begin{aligned} 0 \cdot n &= 0 \cdot n + 0 && \text{V3} \\ &= 0 \cdot n + 0 \cdot n + (-0 \cdot n) && \text{V4} \\ &= (0+0) \cdot n + (-0 \cdot n) && \text{V9} \\ &= 0 \cdot n + (-0 \cdot n) && \text{V3} \\ &= 0. && \text{V4} \end{aligned}$$

EXERCISE 1.2

If $n \in \mathbf{Z}$, then prove that $-n = (-1) \cdot n$.

Solution:

$$\begin{aligned} 0 \cdot n &= 0 && \\ (-1+1) \cdot n &= 0 && \text{V4} \\ (-1) \cdot n + 1 \cdot n &= 0 && \text{V9} \\ (-1) \cdot n + n &= 0 && \text{V7} \\ (-1) \cdot n &= -n. && \end{aligned}$$

THEOREM 1.1: Well-Ordering Axiom (WOA)

Any non-empty subset of the positive integers ($\mathbf{N}$*) has a smallest element.*

There are three main ways of using (WOA) in proofs.

(1) Pick the smallest element in a non-empty subset of $\mathbf{N}$ and show that there is a smallest element.

(2) If a subset of natural numbers contains no smallest element, then the set is empty.

(3) Any statement that implies there is an infinite strictly decreasing sequence of natural numbers must be false. This is called the *Principal of infinite descent*.

THEOREM 1.2: Principal of Mathematical Induction (POMI)

Let $P(n)$ be a statement that depends on $n \in \mathbf{N}$. If $P(0)$ is true and for all $k \in \mathbf{N}$, $P(k)$ implies $P(k+1)$, then $P(n)$ is true for all $n \in \mathbf{N}$.

EXERCISE 1.3

State the Principal of Strong Induction (POSI).

Let $P(n)$ be a statement that depends on $n \in \mathbf{N}$. If $P(0)$ is true and for all $k \in \mathbf{N}$, $P(0), \ldots, P(k)$ implies $P(k+1)$, then $P(n)$ is true for all $n \in \mathbf{N}$.

LECTURE 2
4th May

2 Divisibility

DEFINITION 2.1: Divides in Z

If $a, b \in \mathbf{Z}$, we say a **divides** b, or that a is a factor of b, when $b = ak$ for some $k \in \mathbf{Z}$. We also say at times that a is a divisor of b. When this happens, we write $a \mid b$, and when this does not happen, we write $a \nmid b$.

EXAMPLE 2.1

For example, $-3 \mid 12$, but $6 \nmid 9$. Every $a \mid 0$ since $0 = a \cdot 0$, but $0 \nmid a$ when $a \neq 0$. For otherwise, we would have some k such that

$$0 \neq a = 0 \cdot k = 0.$$

The integers ± 1 divide every integer b. Indeed, $b = 1 \cdot b$ and $b = (-1)(-b)$.

PROPOSITION 2.1

Let $a, b, c, x, y \in \mathbf{Z}$,

(1) $a \mid b \wedge b \mid c \implies a \mid c$.

(2) $c \mid a \wedge c \mid b \implies c \mid (ax + by)$.

(3) $a \mid b \wedge b \neq 0 \implies |a| \leq |b|$.

(4) $a \mid b \wedge b \mid a \implies a = \pm b$.

(5) $a \mid b \implies \pm a \mid \pm b$.

(6) $a \mid b \wedge c \mid d \implies ac \mid bd$.

(7) $\pm 1 \mid a, \ \forall a \in \mathbf{Z}$.

(8) $a \mid 0, \ \forall a \in \mathbf{Z}$.

(9) $a \mid a, \ \forall a \in \mathbf{Z}$.

Proof:

(1) We have $b = ak$ and $c = b\ell$ for some $k, \ell \in \mathbf{Z}$. Then, $c = (ak)\ell = a(k\ell)$, and so $a \mid c$ since $k\ell \in \mathbf{Z}$.

(2) We have $a = ck$ and $b = c\ell$ for some $k, \ell \in \mathbf{Z}$. Then,

$$ax + by = ckx + c\ell y = c(kx + \ell y).$$

And so $c \mid (ax + by)$ since $kx + \ell y \in \mathbf{Z}$.

(3) We have $b = ak$ for some $k \in \mathbf{Z}$. Take absolute values to get $|b| = |a||k|$. Since $b \neq 0$, we get $|k| > 0$, but $k \in \mathbf{Z}$ so $|k| \geq 1$. Hence, $|a| \leq |b|$.

(4) We have $b = ak$ and $a = b\ell$ for some $k, \ell \in \mathbf{Z}$. So, $b = (b\ell)k = b(\ell k)$. If $b = 0$, then $a = 0$ too, whereby $a = \pm b$. If $b \neq 0$, cancel b to get $1 = \ell k$. Thus, $\ell = \pm 1$, and so $a = \pm b$.

(5) We have $b = ak$ for some $k \in \mathbf{Z}$. Then, $-b = a(-k)$ and so $a \mid (-b)$. Also, $b = (-a)(-k)$ and so $-a \mid b$. Continuing for the other two cases, we get that $a \mid \pm b$.

COROLLARY 2.1

Suppose $a \mid b$ and $a \mid c$, then

(1) $a \mid b \pm c$.

(2) $a \mid mb$ for all $m \in \mathbf{Z}$.

Proof: Exercise.
In words, (1) says that if a number divides two other numbers, then it also divides their sum and difference as well. And (2) says that if a number divides another number, then it divides the multiple of the other number.

EXAMPLE 2.2

Prove that if x is an even number, then $x^2 + 2x + 4$ is divisible by 4.

If x is an even number, then $x = 2m$, where $m \in \mathbf{Z}$. $x^2 + 2x + 4$ is divisible by 4 implies $\exists c \in \mathbf{Z}$ such that

$$(2m)^2 + 2(2m) + 4 = 4c.$$

Hence,

$$\begin{aligned}(2m)^2 + 2(2m) + 4 &= 4m^2 + 4m + 4 \\ &= 4(m^2 + m + 1) \\ &= 4c \implies c = m^2 + m + 1.\end{aligned}$$

3 Quotients and Remainders

When divisibility fails, we do look for remainders. Here is an important result about division of integers. It will have a lot of uses; for example, it's the key step in the Euclidean Algorithm, which is used to compute greatest common divisors.

THEOREM 3.1: The Division Algorithm

Let a and b be integers with $a > 0$, then there exists unique integers q, r such that

$$b = aq + r \text{ and } 0 \leq r < a.$$

Proof: The idea is to find the remainder r using Well-Ordering. What is division? Division is successive subtraction. You ought to be able to find r by subtracting a's from b till you can't subtract without going negative. That idea motivates the construction which follows.

Look at the set of integers

$$S = \{b - an : n \in \mathbf{Z} \text{ and } b - an \geq 0\}.$$

In other words, we take b and subtract all possible multiples of a. If we choose $n < \frac{b}{a}$ (there always an integer less than any number), then $an < b$, so $b - an > 0$. This choice of n produces a positive integer $a - bn$ in S. Therefore, S is a non-empty set of non-negative integers and by WOA there is a smallest element $r \in S$. Thus, $r \geq 0$ and $r = b - aq$ for $q \in \mathbf{Z}$. Therefore,

$$b = aq + r.$$

Moreover, if $r \geq a$, then $r - a \geq 0$, so

$$b - aq - a \geq 0 \text{ or } b - a(q + 1) \geq 0,$$

which implies $b - a(q + 1) \in S$, but $r = b - aq > b - a(q + 1)$. This contradicts our assumption that r is the smallest element of S. Therefore,

$$b = aq + r \text{ and } 0 \leq r < a.$$

To show r and q are unique, suppose r' and q' also satisfy these conditions:

$$b = aq' + r' \text{ and } 0 \leq r < a.$$

Also, assume without loss of generality that $r \leq r'$. Then,

$$\begin{aligned} aq + r &= aq' + r', \\ a(q - q') &= r' - r. \end{aligned}$$

Thus, $r' - r$ is a multiple of a. Thus, $\frac{r'-r}{a}$ is an integer and hence $r - r' = 0$ implies $r = r'$. Further, $b(q - q') = 0$ showing that $q = q'$.

DEFINITION 3.1

Let a, b be integers and $a > 0$. We write $b = aq + r$, where $0 \leq r < a$. Then a is called modulus, b is called dividend, q is called quotient, and r is called remainder.

Note that for $a > 0$, the expression $a \mid b$ simply means that in $b = aq + r$ with $r = 0$.

EXAMPLE 3.1

(a) Apply the Division Algorithm to divide 59 by 7.

(b) Apply the Division Algorithm to divide -59 by 7.

1. $59 = 7(8) + 3$.
2. $-59 = 7(-8) + (-3)$.

LECTURE 3

6th May

EXAMPLE 3.2

Prove that if $n \in \mathbf{Z}$, then n^2 does not leave a remainder of 2 or 3 when it's divided by 5.

Solution: We will do this using the Division Algorithm as an illustration. If n is divided by 5, the remainder r satisfies $0 \leq r < 5$. Thus, $r = 0, 1, 2, 3, 4$. Hence, n can have one of the following forms:

$$5q + 0,\ 5q + 1,\ 5q + 2,\ 5q + 3,\ 5q + 4.$$

Check each case:

$$\begin{aligned}
n^2 &= (5q)^2 = 25q^2 = 5(5q^2) + 0 \\
n^2 &= (5q + 1)^2 = 25q^2 + 10q + 1 = 5(5q^2 + 2q) + 1 \\
n^2 &= (5q + 2)^2 = 25q^2 + 20q + 4 = 5(5q^2 + 4q) + 4 \\
n^2 &= (5q + 3)^2 = 25q^2 + 30q + 9 = 5(5q^2 + 6q + 1) + 4 \\
n^2 &= (5q + 4)^2 = 25q^2 + 40q + 16 + 5(5q^2 + 8q + 3) + 1.
\end{aligned}$$

In all cases, dividing n^2 by 5 gave a remainder of 0, 1, or 4.

As an illustration, 191273 can't be perfect square because it leaves a remainder of 3 when it's divided by 5.

4 Greatest Common Divisor

DEFINITION 4.1

Let $a, b \in \mathbf{Z}$ (not both zero). A number $d \in \mathbf{Z}^+$ is called the greatest common divisor (GCD) of a and b if

(1) $d \mid a$ and $d \mid b$,

(2) If $c \mid a$ and $c \mid b$, then $c \mid d$.

In other words, the greatest common divisor of two integers (not both zero) is the largest integer which divides both of them. If a and b are integers (not both 0), the greatest common divisor of a and b is denoted (a, b). The greatest common divisor is sometimes called the greatest common factor or highest common factor.

Here are some easy examples:

- $(8, 6) = 2$;
- $(15, 15) = 15$;
- $(60, 0) = 60$;
- $(18, -15) = 3$.

You were probably able to do the last examples by factoring the numbers in your head. For instance, to find $(8, 6)$, you see that 2 is the only integer bigger than 1 which divides both 8 and 6.

In case $a = b = 0$, it might make sense to say there is no greatest common divisor. Some say that $(0, 0) = 0$, but in any case the issue for us will not arise.

When a and b are small integers, we can find (a, b) by inspection. The problem with this approach is that it requires that you factor the numbers. However, once the numbers get too large — currently, "too large" means "on the order of several hundred digits long" — this approach to finding the greatest common divisor won't work. Fortunately, the Euclidean algorithm computes the greatest common divisor of two numbers without factoring the numbers. We will discuss it after discussing some elementary properties.

PROPOSITION 4.1

Let $a, b \in \mathbf{Z}$ (not both zero). Then,

(1) $(a, b) \geq 1$.

(2) $(a, b) = (|a|, |b|)$.

(3) $(a, b) = (a + kb, b)$*, for any integer* k.

Proof:

(1) Since $1 \mid a$ and $1 \mid b$, (a, b) must be at least as big as 1.

(2) $x \mid a$ if and only if $x \mid -a$; that is, a and $-a$ have the same factors, but $|a|$ is either a or $-a$, so a and $|a|$ have the same factors. Likewise, b and $|b|$ have the same factors. Therefore, x is a common factor of a and b if and only if it's a common factor of $|a|$ and $|b|$. Hence, $(a, b) = (|a|, |b|)$.

(3) First, if x is a common factor of a and b, then $x \mid a$ and $x \mid b$. Then, $x \mid kb$, so $x \mid a + kb$. Thus, x is a common factor of $a + kb$ and b. Likewise, if x is a common factor of $a + kb$ and b, then $x \mid a + kb$ and $x \mid b$ which implies

$$x \mid (a + kb) - kb = a.$$

Thus, x is a common factor of a and b. Therefore,

$$\{\text{common factors of } a \text{ and } b\} = \{\text{common factors of } a + kb \text{ and } b\}.$$

So their largest element are same. The largest element of the first set is (a, b), while the largest element of the second set is $(a + kb, b)$. Therefore, $(a, b) = (a + kb, b)$.

EXAMPLE 4.1

Use the property that $(a, b) = (a + kb, b)$ to compute $(998, 996)$.

Solution: $(998, 996) = (2 + 996, 996) = (2, 996) = 2$.

EXAMPLE 4.2

Prove that if $n \in \mathbf{Z}$, then $(3n + 4, n + 1) = 1$.

$(3n + 4, n + 1) = (3(n + 1) + 1, n + 1) = (1, n + 1)$. Now, $(1, n + 1) \mid 1$, but the only positive integer that divides 1 is 1. Hence, $(1, n + 1) = 1$, and so $(3n + 4, n + 1) = 1$.

REMARK 4.1

In this course, we often use the special case where $(a, b) = 1$.

DEFINITION 4.2

Let $a, b \in \mathbf{Z}$ (not both zero). If $(a, b) = 1$, then we say that a and b are relatively prime or coprime.

For example, 49 and 54 are relatively prime, but 25 and 105 are not.

PROPOSITION 4.2

If $d = (m, n)$*, then* $(\frac{m}{d}, \frac{n}{d}) = 1$.

Proof: Suppose $m = da$ and $n = db$. Then

$$\left(\frac{m}{d}, \frac{n}{d}\right) = (a, b).$$

Suppose that $\ell \in \mathbf{Z}^+$ be a common divisor of m and n. Since d is the greatest common divisor, $d \geq d\ell$. Therefore, $1 \geq \ell$, so $\ell = 1$ (since ℓ is a positive integer). 1 is the only positive common divisor of a and b. Therefore, 1 is the greatest common divisor of a and b, that is,

$$\left(\frac{m}{d}, \frac{n}{d}\right) = (a, b) = 1.$$

5 The Euclidean Algorithm

The main method for calculating the GCD of two integers is the Euclidean Algorithm which is based on the Division Algorithm and Proposition 4.1 (3).

Proposition 4.1 (2) shows that there's no harm in assuming the integers are non-negative.

THEOREM 5.1

Let $a, b \in \mathbf{Z}$ with $b > a > 0$. Use the Division Algorithm repeatedly as follows:

$$\begin{aligned}
&r_1 = b \text{ and } r_2 = a. \\
&r_1 = b = r_2 q_1 + r_3, && 0 \leq r_3 < a = r_2 \\
&r_2 = r_3 q_2 + r_4, && 0 \leq r_4 < r_3 \\
&r_3 = r_4 q_3 + r_5, && 0 \leq r_5 < r_4 \\
&\quad \vdots \\
&r_{n-1} = r_n q_{n-1} + r_{n+1},
\end{aligned}$$

with $r_{n+1} = 0$. Then $(a, b) = (r_2, r_1) = (r_3, r_2) = \cdots = (r_n, 0) = r_n$. We will show that this smallest positive integer r_n is (a, b).

Proof: From Proposition 4.1 (3), we obtain

$$\begin{aligned}
(a, b) = (b, a) &= (r_1, r_2) \\
&= (r_2 q_1 + r_3, r_2) \\
&= (r_3, r_2) \\
&= (r_2, r_3) \\
&= (r_3 q_2 + r_4, r_3) \\
&= (r_4, r_3) \\
&\quad \vdots \\
&= (r_{n+1}, r_n).
\end{aligned}$$

One last step we see that $(a, b) = (r_{n+1}, r_n) = (0, r_n) = r_n$.

Note: The Euclidean Algorithm always terminates as we have the decreasing remainders $r_1 > r_2 > r_3 > \cdots \geq r_n > r_{n+1}$: By WOA sooner or later some remainder becomes 0 because the sequence is bounded below by 0. After n steps, this sequence eventually reaches some smallest positive number r_n.

EXAMPLE 5.1

Use the Euclidean algorithm to compute $(124, 348)$.

Solution: Here are the divisions:

$$\begin{aligned} 348 &= 124 \cdot 2 + 100 \\ 124 &= 100 \cdot 1 + 24, \\ 100 &= 24 \cdot 4 + 4 \\ 24 &= 4 \cdot 6 + 0. \end{aligned}$$

Therefore, $(124, 348) = 4$.
It's easier to remember this visually by arranging the computations in a table. Compare the numbers above to the numbers in the following table:

r_i	q_{i-1}
348	
124	2
100	1
24	4
4	6

The next remainder is 0, so we didn't write it. The successive remainders go in the first column. The successive quotients go in the second column.

To compute the greatest common divisors of three numbers, just compute the greatest common divisor of two numbers at a time.

EXAMPLE 5.2

Compute $(42, 105, 91)$.

Solution: Since $(42, 105) = 21$, so $(42, 105, 91) = \big((42, 105), 91\big) = (21, 91) = 7$.

6 Bézout's Identity

The next result is extremely important, and is often used in proving things about greatest common divisors. First, We will recall a definition from linear algebra.

DEFINITION 6.1

If a and b are numbers, a linear combination of a and b (with integer coefficients) is a number of the form

$$ax + by, \ x, y \in \mathbf{Z}.$$

For instance, $29 = 2 \cdot 10 + 1 \cdot 9$ shows that 29 is a linear combination of 10 and 9. Further, $7 = (-2) \cdot 10 + 3 \cdot 9$ shows that 7 is a linear combination of 10 and 9 as well.

EXAMPLE 6.1

Find the smallest positive integer c that has the form $12x + 8y = c$, where $x, y \in \mathbf{Z}$.

Solution: We can see that $12(1) + 8(-1) = 4$. The question is "can we get a smaller positive integer?" Can we find $x, y \in \mathbf{Z}$ such that $12x+8y = 3$? If we could, we would have $4(3x+2y) = 3$. Since $3x+2y \in \mathbf{Z}$, this would imply that $4 \mid 3$ which is a contradiction. Using the same argument on $12x + 8y = 2$ and $12x + 8y = 1$, we see that none of these are possible. Hence, the smallest positive integer is 4. So, in this case, the smallest positive integer of the form $12x + 8y = c$ is equal to $(12, 8)$.

EXAMPLE 6.2

Find the smallest positive integer c that has the form $28x + 105y = c$, where $x, y \in \mathbf{Z}$.

THEOREM 6.1: Bézout's Identity

Let $a, b \in \mathbf{Z}$ (not both zero). If d is the least positive integer combination of a and b, then d divides every combination of a and b. Furthermore, $d = (a, b)$.

Proof: We know that $ax + by = d > 0$. Now consider some integer combination

$$c = as + bt,\ s, t \in \mathbf{Z}.$$

We want to show that $d \mid c$. By DA, there exists $q, r \in \mathbf{Z}$ such that

$$c = dq + r,\ 0 \leq r < d.$$

Thus,

$$\begin{aligned} 0 &\leq r \\ &= c - dq \\ &= as + bt - (ax + by)q \\ &= a(s - q) + b(t - yq). \end{aligned}$$

We see that r is an integer combination of a and b, which is less than d, and non-negative. Because d is the least positive integer combination of a and b, the only option is that $r = 0$. Hence, $d \mid c$. In particular, $d \mid a$ and $d \mid b$. So d is a common divisor of a and b. We will now show that $d = (a, b)$. Let d' be a common divisor of a and b. Then, $d' \mid a$ and $d' \mid b$. Hence,

$$d' \mid ax + by$$

by property 2 of Proposition 2.1. Thus, we have $d' \mid d$, and by definition of GCD we have $d = (a, b)$.

COROLLARY 6.1

The set of all linear combinations of integers a and b is the set of all multiples of (a, b).

Proof: On one hand,

$$(a, b) \mid ax + by,\ x, y \in \mathbf{Z}.$$

So every linear combination of a and b is a multiple of (a, b). On the other hand,

$$(a, b) = ax + by \text{ so } k(a, b) = a(kx) + b(ky),$$

that is, every multiple of (a, b) is a linear combination of a and b.

COROLLARY 6.2

Two integers a and b are relatively prime if and only if $ax + by = 1$ for some $x, y \in \mathbf{Z}$.

Proof: Suppose a and b are relatively prime; that is, $(a, b) = 1$. By Theorem 1 (Bézout's Identity),

$$ax + by = (a, b) = 1, \text{ for some } x, y \in \mathbf{Z}.$$

On the other hand, suppose $ax + by = 1$ for some $x, y \in \mathbf{Z}$. Since $(a, b) \mid a$ and $(a, b) \mid b$, we have

$$(a, b) \mid ax + by = 1.$$

The only positive integer that divides 1 is 1. Therefore, $(a, b) = 1$

EXERCISE 6.1

Prove that if $n \in \mathbf{Z}$, then $(3n + 17, 2n + 11) = 1$.

Solution: $2(3n + 17) - 3(2n + 11) = 1$, and $(2, 3) = 1$. Therefore, $(3n + 17, 2n + 11) = 1$.

PROPOSITION 6.1

Let $a, b, c \in \mathbf{Z}$. If $(a, b) = 1$, $a \mid c$, and $b \mid c$, then $ab \mid c$.

Proof: Since $a \mid c$ and $b \mid c$, there exists $d, f \in \mathbf{Z}$ such that

$$\begin{aligned} & c = ad \text{ and } c = bf \\ \implies & \frac{c}{a} = d \text{ and } \frac{c}{b} = f. \end{aligned}$$

Further, since a and b are coprime, by Theorem 1 (Bézout's Identity) there exist integers x and y such that

$$ax + by = 1.$$

Thus,

$$\begin{aligned} acx + byc &= c \\ \frac{c}{b}x + \frac{c}{a}y &= \frac{c}{ab} \\ fx + dy &= \frac{c}{ab} \\ ab(fx + dy) &= c, \end{aligned}$$

which implies $ab \mid c$.

PROPOSITION 6.2

Let $a, b, n \in \mathbf{Z}$. If $(n, a) = 1$ and $n \mid ab$, then $n \mid b$.

Proof: By Bézout's Identity, there exists $x, y \in \mathbf{Z}$ such that

$$nx + ay = (n, a) = 1.$$

Multiplying by b gives

$$nxb + ayb = b.$$

Since $n \mid n$ and $n \mid ab$, we get by property 2 of Proposition 2.1 that

$$n \mid nxb + ayb.$$

Therefore, $n \mid b$.

7 The Extended Euclidean Algorithm

We will start by reviewing the Euclidean algorithm, in which the extended Euclidean algorithm is used.

EXAMPLE 7.1

Find $(1914, 899)$. Further, find $x, y \in \mathbf{Z}$ such that $1914x + 899y = 29$.

Solution: We first follow the Euclidean Algorithm,

$$\begin{aligned} 1914 &= 2 \cdot 899 + 116 \\ 899 &= 7 \cdot 116 + 87 \\ 116 &= 1 \cdot 87 + 29 \\ 87 &= 3 \cdot 29 + 0. \end{aligned} \tag{1}$$

We usually write this in tabular form:

r_i	q_{i-1}
1914	899
899	2
116	7
87	1
29	3

So, $(1914, 899) = 29$. We can rewrite the first two equations as:

$$1914 - 2 \cdot 899 = 116. \tag{2}$$

$$899 - 7 \cdot 116 = 87. \tag{3}$$

Substitute (2) into (3) to get

$$\begin{aligned} 899 - 7 \cdot (1914 - 2 \cdot 899) &= 87. \\ -7 \cdot 1914 + 15 \cdot 899 &= 87. \end{aligned} \tag{4}$$

We can now rewrite the third equation of (1) as:

$$116 - 1 \cdot 87 = 29. \tag{5}$$

Substituting (2) and (4) into (5) gives

$$\begin{aligned} (1914 - 2 \cdot 899) - 1 \cdot (-7 \cdot 1914 + 15 \cdot 899) &= 29 \\ 8 \cdot 1914 - 17 \cdot 899 &= 29. \end{aligned}$$

Thus, $x = 8$ and $y = 17$.

The above procedure is painful to carry out by hand, or even with a basic calculator. Let's explore a method of calculations, i.e., an algorithm, for solving the equation

$$ax + by = (a, b), \ x, y \in \mathbf{Z}.$$

It is called a backward recurrence, and is due to S. P. Glasby. It will look a little complicated, but you'll see that it's really easy to use in practice.

THEOREM 7.1

Let $a, b \in \mathbf{Z}^+$ with $b > a$. Define

$$\begin{array}{ll} r_1 = b & r_2 = a \\ s_1 = 1 & s_2 = 0 \\ t_1 = 0 & t_2 = 1 \end{array}$$

and sequences as:

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_{i-1} r_i \\ s_{i+1} &= s_{i-1} - q_{i-1} s_i \\ t_{i+1} &= t_{i-1} - q_{i-1} t_i. \end{aligned}$$

Then, for $i \in \mathbf{Z}^+$, we have

$$bs_i + at_i = r_i.$$

In particular, if $r_n = (a, b)$, then

$$bs_n + at_n = (a, b).$$

Proof: Use induction on n.

EXAMPLE 7.2

Find $x, y \in \mathbf{Z}$ such that $1914x + 899y = (1914, 899)$.

Solution:

r_i	q_{i-1}	s_i	t_i	Check
1914		1	0	
899	2	0	1	
116	7	1	-2	$1(1914) + (-2)(899) = 116$
87	1	-7	15	$(-7)(1914) + 15(899) = 87$
29	3	8	-17	$8(1914) + (-17)(899) = 29$

You can fill the columns of s_i and t_i for $i \geq 3$ with

$$\begin{aligned} \text{next } s &= \text{previous to last } s - (\text{last } q)(\text{last } s), \\ \text{next } t &= \text{previous to last } t - (\text{last } q)(\text{last } t). \end{aligned}$$

EXERCISE 7.1

Compute $(187, 102)$ and express it as a linear combination of 187 and 102.

Solution: We first follow the Euclidean Algorithm,

r_i	q_{i-1}	s_i	t_i	Check
187		1	0	
102	1	0	1	
85	1	1	-1	$1(187) + (-1)(102) = 85$
17	5	-1	2	$(-1)(187) + (2)(102) = 17$

Therefore,

$$187 \cdot (-1) + 102 \cdot 2 = (187, 102) = 17.$$

EXERCISE 7.2

Find the smallest c, and x, y such that $c = 246x + 194y$.

Solution:

r_i	q_{i-1}	s_i	t_i	Check
246		1	0	
194	1	0	1	
52	3	1	-1	$1(246) + (-1)(194) = 52$
38	1	-3	4	$(-3)(246) + (4)(194) = 38$
14	2	4	-5	$(4)(246) + (-5)(194) = 14$
10	1	-11	14	$(-11)(246) + (14)(194) = 10$
4	2	15	-19	$(15)(246) + (-19)(194) = 4$
2	2	-41	52	$(-41)(246) + (52)(194) = 2.$

Thus, $x = -41$, $y = 52$, and $c = 2$.

EXERCISE 7.3

Find $x, y \in \mathbf{Z}$ such that $126x + 91y = (126, 91)$.

LECTURE 5
11th May

8 Diophantine Equations

A polynomial equation in several variables in which we are only interested in integer solutions is called a Diophantine equation. Diophantine equations are named after the 3rd century mathematician Diophantus of Alexandria who wrote a series of books called Arithmetica wherein he raised the matter of solving the equations now named in his honour.

EXAMPLE 8.1

Let $a, b, c, n \in \mathbf{Z}$. Some famous Diophantine equations are:

- $ax + by + c$: Linear Diophantine equation in two variables.
- $x^2 + y^2 = z^2$: Pythagorean Triple.
- $x^2 - dy^2 \pm 1$, where $d \in \mathbf{Z}^+$ is non-square: Pell's Equation.
- $ax^n + by^n = cz^n$, where $n \in \mathbf{Z}$, $n \geq 3$: Fermat type Equation.

For now, we will just look at linear Diophantine equation in two variables,

$$ax + by = c,$$

where a, b, c are fixed integers and x, y are integer variables. When analyzing equations, we would like to answer the following questions.

(1) Does a solution exist?

(2) If solutions exist, how many of them exist? (finite, infinite, countably, or uncountably many)

(3) What are the solutions?

(4) Are there any algorithms which generates the solution(s)?

We address the same questions when analyzing Diophantine equations.

THEOREM 8.1

Let $a, b, c \in \mathbf{Z}$. Let (x, y) be a pair of integers satisfying the Diophantine equation

$$ax + by = c.$$

(a) If $(a, b) \nmid c$, then no solutions exist for $ax + by = c$.

(b) If $(a, b) = d \mid c$, then there are infinitely many solutions of the form

$$x' = x_0 - \frac{b}{d}t,$$
$$y' = y_0 + \frac{a}{d}t,$$

where the pair (x_0, y_0) is a particular solution to the equation $ax + by = c$, and $t \in \mathbf{Z}$.

Proof:

(a) Suppose $(a, b) \nmid c$. Let the pair (x', y') be solutions of the equation $ax + by = c$; that is, $ax' + by' = c$. Since $(a, b) \mid a$ and $(a, b) \mid b$,

$$(a, b) \mid ax + by = c$$

by property 2 of Proposition 2.1, which is a contradiction. Hence, no solution exists.

(b) Suppose $(a, b) = d \mid c$, then $c = dk$ for some $k \in \mathbf{Z}$. By Bézout's Identity, there are integers m, n such that

$$am + bn = d = (a, b).$$

Then,

$$amk + bnk = dk = c.$$

Hence, the pair (mk, nk) is a solution.

Suppose the pair (x_0, y_0) is a particular solution. Then,

$$a\left(x_0 - \frac{b}{d}t\right) + b\left(y_0 + \frac{a}{d}t\right) = \frac{ab}{d}t - \frac{ab}{d}t + (ax_0 + by_0) = 0 + c = c,$$

which proves that the pair $(x_0 - \frac{b}{d}t, y_0 + \frac{a}{d}t)$ is a solution for every $t \in \mathbf{Z}$.

Let (x', y') and (x_0, y_0) be the pairs such that $ax' + by' = c$ and $ax_0 + by_0 = c$. Hence,

$$a(x_0 - x') = b(y' - y_0)$$
$$\implies \frac{a(x_0 - x')}{d} = \frac{b(y' - y_0)}{d}.$$

Now, $\frac{b}{d} \mid \frac{a}{d}(x_0 - x')$. However, $(\frac{a}{d}, \frac{b}{d}) = 1$ by Proposition 4.2. Therefore,

$$\frac{b}{d} \mid x_0 - x',$$

(using Proposition 6.2) would imply

$$x_0 - x' = t\frac{b}{d}, \text{ for some } t \in \mathbf{Z}.$$

Thus,

$$x' = x_0 - \frac{b}{d}t.$$

Substituting $x_0 - x' = t\frac{b}{d}$ into the equation $a(x_0 - x) = b(y - y_0)$, we see that

$$y' = y_0 + \frac{a}{d}t.$$

EXAMPLE 8.2

Solve the Diophantine equation $6x + 9y = 5$.

Solution: Since $(9, 6) = 3 \nmid 5$, the equation has no solution.

EXAMPLE 8.3

Find all the solutions (x, y) to the Diophantine equation

$$11x + 13y = 369.$$

Solution: Since $(11, 13) = 1 \mid 369$, there are infinitely many solutions. It is hard to guess the particular solution, so we will use the EEA:

r_i	q_{i-1}	s_i	t_i	Check
13		1	0	
11	1	0	1	
2	5	1	-1	$(1)(13) + (-1)(11) = 2$
1	2	-5	6	$(-5)(13) + (6)(11) = 1$

$$(11)(6) + (13)(-5) = 1$$
$$(11)(2214) + (13)(-1845) = 369.$$

So, $(2214, -1845)$ is a particular solution. The general solution is

$$x = 2214 - 13t, \quad y = -1845 + 11t, \ t \in \mathbf{Z}.$$

EXERCISE 8.1

Find all solutions of the linear Diophantine equation

$$132x + 84y = 144.$$

Solution:

r_i	q_{i-1}	s_i	t_i	Check
132		1	0	
84	1	0	1	
48	1	1	-1	$132(1) + 84(-1) = 48$
36	1	-1	2	$132(-1) + 84(2) = 36$
12	1	2	-3	$132(2) + 84(-3) = 12$

Hence,

$$132(2) + 84(-3) = 12$$
$$132(2 \cdot 12) + 84(-3 \cdot 12) = 12 \cdot 12$$
$$132 \cdot 24 + 84 \cdot (-36) = 144.$$

So, $(x_0, y_0) = (24, -36)$ is a particular solution. The general solution is:

$$x = x_0 - \frac{b}{d}t = 24 - \frac{84}{12}t = 24 - 7t,$$
$$y = y_0 - \frac{a}{d}t = -36 + \frac{132}{12}t = -36 + 11t,\ t \in \mathbf{Z}$$

Consider a 3-variable equation

$$ax + by + cz = d.$$

The equation has solutions if $(a, b, c) \mid d$. If it has a solution, there will be infinitely many, determined by two integer parameters.

EXERCISE 8.2

Find the general solution to the Diophantine equation

$$8x + 14y + 5z = 11.$$

Solution:

$$2(4x + 7y) + 5z = 11.$$

Let $w = 4x + 7y$, so

$$2w + 5z = 11.$$

Now, $w = -22$ and $z = 11$ is a particular solution, so

$$w = -22 + 5s, \quad z = 11 - 2s,\ s \in \mathbf{Z}.$$

Then,

$$4x + 7y = w = -22 + 5s.$$

$x = -44 + 10s$ and $y = 22 - 5s$ is a particular solution. The general solution is

$$x = -44 + 10s + 7t$$
$$y = 22 - 5s - 4t$$
$$z = 11 - 2s.$$

9 Prime Numbers

DEFINITION 9.1

An integer p is called prime when $p \neq 0$, $p \neq \pm 1$, and the only factors that p have are ± 1 and $\pm p$.

Clearly, p is prime if and only if p is prime. To avoid this double counting of primes we shall work only with positive primes and to be brief we shall usually omit the word "positive."

LEMMA 9.1

Every integer greater than 1 is divisible by at least one prime.

Proof: Let's use induction. To begin with, the result is true for $n = 2$ since 2 is prime.
Suppose $2, 3, 4, \ldots, k-1$ is divisible by at least one prime. If k is prime, it is divisible by a prime — namely itself! If k is composite, then $k = ab$, where $1 < a < k$ and $1 < b < k$. Since a and b are among the integers $2, 3, 4, \ldots, k-1$, each of them is divisible by at least one prime; that is, there exists p such that $p \mid a$ and $a \mid k$ implies $p \mid k$, so k has a prime factor as well. This shows that the result is true for all $n > 1$

by induction.

And now comes a classic discovery and its proof occur as Proposition 20 in Book 9 of Euclid's Elements.

PROPOSITION 9.1: Euclid's Theorem

There are infinitely many prime numbers.

Proof: Suppose on the contrary that there are only finitely many primes $p_1, \ldots, p_n$. Look at

$$p_1 p_2 \cdots p_n + 1.$$

This number is not divisible by any of the primes $p_1, \ldots, p_n$ because it leaves the remainder of 1 when divided by any of them. According to Lemma 1, there exists a new prime number q such that $q \mid p_1 p_2 \cdots p_n + 1$, a contradiction. This contradiction implies that there cannot be finitely many primes; that is, there are infinitely many.

The special thing about primes is that there is only one way to write an integer into primes. Ambiguous factoring such as

$$30 = (6)(5) = (15)(2)$$

do not occur when only primes are involved in the factors. To prove the Unique factorization, we need what we can only be called the signature property of primes.

PROPOSITION 9.2: Euclid's Lemma

Let $a, b \in \mathbf{Z}$. If p is a prime number and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: Assume $p \mid ab$, then there exists $n \in \mathbf{Z}$ such that $pn = ab$. Further, assume $p \nmid a$. Since a is not a multiple of p and the only factors of p are 1 and p, we must have $(a, p) = 1$. So by Bézout's Identity, there exists $x, y \in \mathbf{Z}$ such that

$$\begin{aligned} ax + py &= 1. \\ abx + pby &= b. \\ pnx + pby &= b. \\ p(nx + by) &= b. \end{aligned}$$

Since $nx + by \in \mathbf{Z}$, $p \mid b$.

Note that Proposition 9.2 fails when p is not a prime. For instance $6 \mid 12 = (3)(4)$, but $6 \nmid 3$ and $6 \nmid 4$.

LECTURE 7
16th May

PROPOSITION 9.3

Let $n, a_1, \ldots, a_n \in \mathbf{Z}^+$. If $p \mid a_1 \cdots a_n$, then there exists some $i \in [1, n]$ such that $p \mid a_i$.

Proof: If $n = 1$, then $p \mid a_1$ and we are done. Assume $p \mid a_1 \cdots a_k$ implies there exists some $i \in [1, n]$ such that $p \mid a_i$. Then, by Euclid's Lemma, $p \mid a_1 \cdots a_{k+1}$ implies $p \mid a_{k+1}$ or $p \mid a_1 \cdots a_k$. If $p \mid a_{k+1}$, then we are done. If $p \mid a_1 \cdots a_k$, then we are also done by the inductive hypothesis. Hence, the result is true for $n = k + 1$ which implies the result is true for $n \in \mathbf{Z}^+$.

THEOREM 9.1: Fundamental Theorem of Arithmetic (FTA)

Every integer greater than 1 *can be written uniquely (up to ordering) as the product of primes.*

Proof: We will start by proving that every positive integer greater than 1 can be written as a product of primes. Let S denote the collection of all positive integers greater than 1 that cannot be written as a product of primes. Suppose that S is non-empty. Since $S \subset \mathbf{N}$ and by WOA, there exists a smallest element of S, say n. Then n cannot be a prime as otherwise it would not be in S. Thus, n is composite, say $n = ab$. Since a and b are both less than n, they can be written as products of prime numbers. Say

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \qquad b = q_1^{\beta_1} \cdots q_\ell^{\beta_\ell}.$$

But then,

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1 \beta_1 \cdots q_1^{\beta_1} \cdots q_\ell^{\beta_\ell},$$

which is a contradiction. This means that S is empty. So every integer greater that 1 is a product of primes. To prove uniqueness, consider two distinct prime factorizations of n as

$$p_1^{\alpha_1} \cdots p_k^{\alpha_k} = q_1 \beta_1 \cdots q_1^{\beta_1} \cdots q_\ell^{\beta_\ell}.$$

Note here the p's are distinct primes, the q's are distinct primes, and all the exponents are greater than or equal to 1.
Consider p_1. It divides the left side, so it divides the right side. Using Proposition 1 $p_1 \mid q_i^{\beta_i}$ for some i which implies $p_1 = q_i$ since they are both prime numbers. To avoid a mess, renumber the q's so q_i becomes q_1 and vice versa. Thus, $p_1 = q_1$, and the equation reads

$$p_1^{\alpha_1} \cdots p_k^{\alpha_k} = p_1 \beta_1 \cdots q_1^{\beta_1} \cdots q_\ell^{\beta_\ell}.$$

If $\alpha_1 > \beta_1$, then we have

$$p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}.$$

This is impossible since now p_1 divides the left side, but not the right. For the same reason, $\alpha < \beta_1$ is impossible. It follows that $\alpha_1 = \beta_1$, so we can cancel the p_1's off both sides leaving

$$p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}.$$

Keep going. At each stage, we pair up a power of p with a power of q, and the preceding argument shows the powers are equal. We can't wind up with any primes left over at the end, or else I'd have a product of primes equals to 1. So everything must have paired up, and the original factorizations were the same (except possibly for the order of the factors).

EXAMPLE 9.1

Consider the set H of all numbers of the form $4n + 1$ where n is a non-negative integer, that is,

$$H = \{1, 5, 9, 13, 17, 21, 25, 29, \ldots\}.$$

These numbers are called **Hilbert** numbers. Observe that H is closed under multiplication, that is, if we multiply any two Hilbert numbers, we get another Hilbert number. Indeed,

$$(4x + 1)(4y + 1) = 4(4xy + x + y) + 1.$$

A number in H, other than 1, that has no divisor in H other than 1 and itself is called Hilbert prime. The first few Hilbert Primes are 5, 9, 13, 17, 21, and 29. Note 25 is a Hilbert composite because 5 is in the set. The set H does not have unique prime factorization. Indeed, $693 = (9)(77) = (21)(33)$.

EXAMPLE 9.2: Why is 1 is not a prime in Z?

Some might argue that the integer 1 deserve to be called a prime. After all, it cannot be factored down any further. However, if we allow 1 to be prime then Unique factorization goes out the window. Indeed, we can factor the integer 1 from any integer a as much as we like:

$$a = (1)(1)(1)\cdots(1)(a).$$

True prime don't do that. The number of times they appear in the Unique factorization of a is unique. That's what allows the factorization to be called "unique." Better to leave 1 out of the basket of integers known as primes.

10 Gaussian Integer

The Gaussian integers were introduced by Gauss in 1832.

DEFINITION 10.1: Gaussian Integers

The set

$$\mathbf{Z}[i] = \{x + iy : x, y \in \mathbf{Z} \wedge i^2 = -1\}$$

is called the set of **Gaussian integers**.

Observe that $\mathbf{Z} \subset \mathbf{Z}[i]$ since $a + 0i \in \mathbf{Z}$.

DEFINITION 10.2: Axioms in $\mathbf{Z}[i]$

The Gaussian integers have all the same important properties as $\mathbf{Z}$. This means that $\in \mathbf{Z}[i]$ satisfies the following axioms:

V1 $\mathbf{Z}[i]$ has operations $+$ (addition) and $\cdot$ (multiplication). It is closed under these operations, in that if $a, b \in \mathbf{Z}[i]$, then $a + b \in \mathbf{Z}[i]$ and $a \cdot b \in \mathbf{Z}[i]$.

V2 Addition is associative: If $a, b, c \in \mathbf{Z}[i]$, then

$$a + (b + c) = (a + b) + c.$$

V3 There is an additive identity $0 \in \mathbf{Z}$: For all $a \in \mathbf{Z}[i]$,

$$a + 0 = 0 + a = a.$$

V4 Every element has an additive inverse: If $a \in \mathbf{Z}[i]$, there is an element $-a \in \mathbf{Z}[i]$ such that

$$a + (-a) = 0 \text{ and } (-a) + a = 0.$$

V5 Addition is commutative: If $a, b \in \mathbf{Z}[i]$, then

$$a + b = b + a.$$

V6 Multiplication is associative: If $a, b, c \in \mathbf{Z}[i]$, then

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

V7 There is a multiplicative identity $1 \in \mathbf{Z}[i]$: For all $a \in \mathbf{Z}[i]$,

$$a \cdot 1 = a = 1 \cdot a.$$

V8 Multiplication is commutative: If $a, b \in \mathbf{Z}[i]$, then

$$a \cdot b = b \cdot a.$$

V9 The Distributive Laws hold: If $a, b, c \in \mathbf{Z}[i]$, then

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

V10 There are no zero divisors: If $a, b \in \mathbf{Z}[i]$ and $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

Clearly, $\mathbf{Z}[i]$ is an integral domain.

Our goal is to determine "whether the Gaussian integers have unique prime factorization or not?" To do this, we try to mimic what we did in the integers.

Notice that it is uncommon for the division of one Gaussian Integer by another to yield a Gaussian Integer as its quotient (the analogous statement in $\mathbf{Z}$ is also seen to be true). For example, we can divide these two elements in $\mathbf{C}$ to find:

$$\frac{1+6i}{4+7i} = \frac{46}{75} + \frac{17}{75}i$$

is not a Gaussian integer. However, we find that some particular divisions do yield a quotient in $\mathbf{Z}[i]$:

$$\frac{2+5i}{i} = 5 - 2i$$
$$\frac{-6+8i}{1+7i} = 1 + i.$$

To further understand this divisibility behaviour, we develop a tool to measure the size of a Gaussian integer called the **norm** so that we have a meaning to be bigger or smaller in the Gaussian integers.

DEFINITION 10.3: Norm

If $z = x + iy \in \mathbf{Z}[i]$, then we define the norm of z by

$$N(z) = x^2 + y^2 = z\bar{z}.$$

EXAMPLE 10.1

We have

$$N(1) = 1^2 + 0^2 = 1$$
$$N(-2i) = 0 + (-2)^2 = 4$$
$$N(-3 + 2i) = (-3)^2 + 2^2 = 13.$$

So, by one Gaussian integer z being smaller than another Gaussian integer w, we mean that $N(z) < N(w)$.

However before we go back to trying to figure out the Division in Gaussian integers, it makes sense to think about the properties of the norm.

EXERCISE 10.1

Create a bunch of your own examples with the purpose of trying to figure out what properties the norm might have.

THEOREM 10.1

If $z, w \in \mathbf{Z}[i]$, then

(1) $N(z) \in \mathbf{N} \cup \{0\}$.

(2) $N(z) = 0 \iff z = 0$.

(3) $N(zw) = N(z)N(w)$.

11 Divisibility and units in $\mathbf{Z}[i]$

We now define divisibility in $\mathbf{Z}[i]$ analogously to divisibility in $\mathbf{Z}$, using the norm's multiplicativity to great effect.

DEFINITION 11.1: Divides in $\mathbf{Z}[i]$

If $\alpha, \beta \in \mathbf{Z}[i]$, we say that z divides w, and write $z \mid w$, provided that $w = zX$ for some $X \in \mathbf{Z}[i]$. In this case, w is a multiple of z and z is a factor of w.

EXAMPLE 11.1

$1 + 2i$ divides $5 + 0i$ in $\mathbf{Z}[i]$ because

$$5 + 0i = (1 + 2i)(1 - 2i).$$

Let us collect some facts and definitions regarding divisibility. The next theorem turns out to be very useful.

THEOREM 11.1

If $z \mid w$ in $\mathbf{Z}[i]$, then $N(z) \mid N(w)$ in $\mathbf{Z}$.

EXERCISE 11.1

Find $q, r \in \mathbf{Z}[i]$ such that $w = qz + r$ for each pair $w, z \in \mathbf{Z}[i]$.

(1) $w = 3 + 7i$, $z = 4 + 5i$.

(2) $w = 7 - 3i$, $z = 2 + 7i$.

(3) $w = 1 + 2i$, $z = 3 - i$.

Solution:

Exercise 11.1 shows that unlike in $\mathbf{Z}$, the quotient and remainder are not unique in the Gaussian integers.

LECTURE 8
18th May

12 Primes in $\mathbf{Z}[i]$

Recall that our goal here is to look at prime factorizations in $\mathbf{Z}[i]$. So, we are in need to define primes in $\mathbf{Z}[i]$.

In $\mathbf{Z}[i]$, we classified every number into one of four types: zero, unit, prime, or composite. We do the same for $\mathbf{Z}[i]$. The first two definitions are the same: we have a number 0, and a number $z \in \mathbf{Z}[i]$ is a unit, if there exists a number $w \in \mathbf{Z}[i]$, such that $zw = 1$; that is, z must divide 1. However, in $\mathbf{Z}[i]$, our definitions for primes and composite numbers are not good. In $\mathbf{Z}$, we talked about positive divisors, but we do not have a concept of positive or negative numbers in $\mathbf{Z}[i]$. Therefore, we need to come up with better definitions for prime and composite numbers. To do this, we must first make sure that we understand units.

DEFINITION 12.1: Unit in $\mathbf{Z}[i]$

If z is a **unit** in $\mathbf{Z}[i]$, then there exists $w \in \mathbf{Z}[i]$ such that $zw = 1$.

EXAMPLE 12.1

Find all units in $\mathbf{Z}$.

THEOREM 12.1

A number z is a unit in $\mathbf{Z}[i]$ if and only if $N(z) = 1$.

Proof: If z is a unit in $\mathbf{Z}[i]$, then by definition there exists $w \in \mathbf{Z}[i]$ such that $zw = 1$. Hence, we have

$$N(zw) = N(1)$$
$$N(z)N(w) = 1.$$

Thus, $N(z) \mid 1$ in $\mathbf{Z}$. Therefore, $N(z) = 1$ since $N(z) \in \mathbf{N}$.
On the other hand, if $z = x + iy \in \mathbf{Z}[i]$ such that $N(z) = 1$, then $x^2 + y^2 = 1$. Since $x, y \in \mathbf{Z}$, the only possibilities are $z = 1 + 0i$, $z = -1 + 0i$, $z = 0 + i$, and $z = 0 - i$. It is easy to verify that each of these numbers are units in $\mathbf{Z}[i]$.

DEFINITION 12.2: Prime in $\mathbf{Z}[i]$

Let $z \in \mathbf{Z}[i]$. z is called a **prime** in $\mathbf{Z}[i]$ if

(i) z is not a unit, and

(ii) any factorization $z = wu$ forces w or u to be a unit in $\mathbf{Z}[i]$.

EXERCISE 12.1

Are all prime numbers in $\mathbf{Z}$ also prime numbers in $\mathbf{Z}[i]$?

EXAMPLE 12.2

The integer 2 is a prime in $\mathbf{Z}$, but is not a prime in $\mathbf{Z}[i]$ since $2 = (1 + i)(1 - i)$, and neither $1 + i$ nor $1 - i$ is a unit. The number 3 is a prime in both $\mathbf{Z}$ and $\mathbf{Z}[i]$. Suppose that $3 = zw$ for some $z, w \in \mathbf{Z}[i]$. Then,

$$N(zw) = N(3) = 9$$
$$N(z)N(w) = 9,$$

which means that $N(z) \mid 9$ and $N(w) \mid 9$. Hence, $N(z)$ equals one of 1, 3, or 9.

- If $N(z) = 1$, then z must be a unit by Theorem 12.1.
- If $N(z) = 3$, let $z = x + iy$, then
$$3 = N(z) = x^2 + y^2.$$
If $y \neq 0$, then $x^2 + y^2 \neq 3$. If $y = 0$, then $x^2 = 3$ is a perfect square not equal to 3. Therefore, $N(z) \neq 3$. Analogously, $N(w) \neq 3$.
- If $N(z) = 9$, then $N(w) = 1$, and as seen already this forces w to be unit.

EXERCISE 12.2

Prove that 7 is prime in $\mathbf{Z}[i]$.

Solution: Note that

$$N(zw) = N(7) = 49 \iff N(z)N(w) = 49,$$

which means that $N(z) \mid 49$ and $N(w) \mid 49$. Hence, $N(z)$ equals to one of 1, 7, or 49.

- If $N(z) = 1$, then z must be a unit by Theorem.
- If $N(z) = 7$, let $z = x + iy$, then
$$7 = x^2 + y^2.$$
If $y \neq 0$, then $x^2 + y^2 \neq 7$. If $y = 0$, then $x^2 = 7$ is a perfect square not equal to 3. Therefore, $N(z) \neq 3$. Analogously, $N(w) \neq 3$.
- If $N(z) = 49$, then $N(w) = 1$, and as seen already this forces w to be a unit.

EXERCISE 12.3

Prove that $2 + i$ is prime in $\mathbf{Z}[i]$.

Solution: Note that

$$N(zw) = N(2 + i) = 3^2 + 1^2 = 10 \iff N(z)N(w) = 10,$$

which means that $N(z) \mid 10$ and $N(w) \mid 10$. Hence, $N(z)$ equals to one of 1, 2, 5, or 10.

- If $N(z) = 1$, then z must be a unit by Theorem.
- If $N(z) = 2$, let $z = x + iy$, then
$$2 = x^2 + y^2.$$
If $y \neq 0$, then $x^2 + y^2 \neq 2$. If $y = 0$, then $x^2 = 2$ is a perfect square not equal to 2. Therefore, $N(z) \neq 2$. Analogously, $N(w) \neq 2$.
- If $N(z) = 5$, let $z = x + iy$, then
$$5 = x^2 + y^2.$$
If $y \neq 0$, then $x^2 + y^2 \neq 5$. If $y = 0$, then $x^2 = 5$ is a perfect square not equal to 5. Therefore, $N(z) \neq 5$. Analogously, $N(w) \neq 5$.
- If $N(z) = 10$, then $N(w) = 1$, and as seen already this forces w to be a unit.

EXERCISE 12.4

Make a conjecture to which primes in $\mathbf{Z}$ are also prime in $\mathbf{Z}[i]$.

LECTURE 9

20th May

Next, we want to look at the GCD in $\mathbf{Z}[i]$.

DEFINITION 12.3: Greatest Common divisor in $\mathbf{Z}[i]$

Let $z, w \in \mathbf{Z}[i]$ not both zero. We define the set of common divisors of z and w as

$$\{X \in \mathbf{Z}[i] : X \mid z \wedge X \mid w\}.$$

There will be an element $d \in \mathbf{Z}[i]$ with maximal norm in this set, and that we call the **greatest common**

divisor of z and w; that is, if $c \mid z$ and $c \mid w$, then $N(d) \geq N(c)$.

The Euclidean Algorithm also works for finding a GCD of two numbers in $\mathbf{Z}[i]$.

EXAMPLE 12.3

Use the Euclidean Algorithm to find a GCD of $z = 11 + 3i$ and $w = 1 + 8i$.

Solution: We have

$$\begin{aligned} 11 + 3i &= (1 - i)(1 + 8i) + 2 - 4i \\ 1 + 8i &= (-2 + i)(2 - 4i) + 1 - 2i \\ 2 - 4i &= 2(1 - 2i) + 0. \end{aligned}$$

Therefore, a GCD of $z = 11 + 3i$ and $w = 1 + 8i$ is $1 - 2i$.

EXERCISE 12.5

Use the Euclidean Algorithm to find a GCD of $z = 3 + 10i$ and $z = 2 + 4i$.

Solution:

$$\begin{aligned} \frac{3 + 10i}{2 + 4i} &= \frac{23 + 4i}{10} \sim 2 + 0i \\ \frac{2 + 4i}{-1 + 2i} &= 1.2 - 1.6i \sim 1 - 2i \\ \frac{-1 + 2i}{-1} &= 1 - 2i. \end{aligned}$$

$$\begin{aligned} 3 + 10i &= (2 + 0i)(2 + 4i) + (-1 + 2i) \\ 2 + 4i &= (1 - 2i)(-1 + 2i) + (-1) \\ -1 + 2i &= (1 - 2i)(-1) + 0. \end{aligned}$$

So, $(3 + 10i, 2 + 4i) = 1 - 2i$.

EXERCISE 12.6

What are all GCD of $w = 11 + 3i$ and $z = 1 + 8i$?

We now prove Bezout's Identity in $\mathbf{Z}[i]$. You should be looking and thinking about the difference between this proof and the proof of Bezout's Identity in $\mathbf{Z}$.

THEOREM 12.2: Bezout's Identity in $\mathbf{Z}[i]$

Let $z, w \in \mathbf{Z}[i]$ not both zero. If d is a GCD of z, then for any $x, y \in \mathbf{Z}[i]$, $d \mid (zx + wy)$. Moreover, there exists $s, t \in \mathbf{Z}[i]$ such that

$$zs + wt = d.$$

Proof: Let $c = zx + wy$ for some $x, y \in \mathbf{Z}[i]$. By definition of GCD, we have $z = da$ and $w = db$ for some $a, b \in \mathbf{Z}[i]$. Thus,

$$c = (da)x + (db)y = d(ax + by).$$

Since $ax + by \in \mathbf{Z}[i]$, we have $d \mid c$ in $\mathbf{Z}[i]$.
Let $S = \{N(zs + wt) : s, t \in \mathbf{Z}[i] \wedge N(zs + wt) > 0\}$. Observe that S is non-empty since z and w are both non-zero. Also, $S \subset \mathbf{N}$ since $N(zs + wt) \in \mathbf{N}$, so we can pick the smallest element in S by WOA.

Let $d = zs + wt$ be the number in $\mathbf{Z}[i]$ corresponding to the smallest element in S.
By the Division Algorithm, there exists $q, r \in \mathbf{Z}[i]$ such that $z = qd + r$, where $N(r) < N(d)$. Then,

$$r = z - qd = z - (zs + wt)q = z(1 - sq) + w(-tq).$$

If $N(r) > 0$, then $N(r) \in S$ with $N(r) < N(d)$ which is a contradiction. So, we must have $N(r) = 0$ which implies $r = 0$. Thus, $d \mid z$. Similarly, we can show that $d \mid w$.
Let c be any other common divisor of z and w. Then, there exists $s', t' \in \mathbf{Z}[i]$ such that $z = cs'$ and $w = ct'$. Hence,

$$d = zs + wt = cs's + ct't = c(s's + t't).$$

So, $c \mid d$ and hence $N(c) \leq N(d)$.

The Extended Euclidean Algorithm also works in $\mathbf{Z}[i]$.

EXAMPLE 12.4

Let $z = 3 + 10i$ and $w = 2 + 4i$. Find $s, t \in \mathbf{Z}[i]$ such that $zs + wt$ equals to a GCD of z and w.

EXAMPLE 12.5

Let $z = 32 + 9i$ and $w = 4 + 11i$. Find $s, t \in \mathbf{Z}[i]$ such that $zs + wt$ equals to a GCD of z and w.

EXERCISE 12.7

Let $z = 11 + 3i$ and $w = 1 + 8i$. Find $s, t \in \mathbf{Z}[i]$ such that $zs + wt$ equals to a GCD of z and w.

Solution: We know that a GCD of z and w is $1 - 2i$. We want to find $x, y \in \mathbf{Z}[i]$ such that

$$(11 + 3i)s + (1 + 8i)t = 1 - 2i.$$

EEA:

r_i	q_{i-1}	s_i	t_i	Check
$11 + 3i$		1	0	
$1 + 8i$	$1 - i$	0	1	
$2 - 4i$	$-2 + i$	1	$-1 + i$	$(1)(11 + 3i) + (-1 + i)(1 + 8i) = 2 - 4i$
$1 - 2i$	2	$2 - i$	$3i$	$(2 - i)(11 + 3i) + (3i)(1 + 8i) = 1 - 2i$

So, $(2 - i, 3i)$ is a particular solution.

Since GCDs are not unique, we define relatively prime in terms of the norm.

DEFINITION 12.4

Two numbers $z, w \in \mathbf{Z}[i]$ are relatively prime (coprime) if there exists $x, y \in \mathbf{Z}[i]$ such that

$$N(zx + wy) = 1.$$

Finally, we prove the analogue of Euclid's Lemma for $\mathbf{Z}[i]$.

PROPOSITION 12.1: Euclid's Lemma in $\mathbf{Z}[i]$

If p is a prime in $\mathbf{Z}[i]$ and $p \mid zw$, then $p \mid z$ or $p \mid w$.

Proof: Suppose $p \mid zw$, so there exists $\ell \in \mathbf{Z}[i]$ such that $zw = \ell p$. Suppose $p \nmid z$. Let d be the GCD of p and z. So

$$d = zs + pt \text{ for some } s, t \in \mathbf{Z}[i] \text{ and } u \mid p \text{ and } u \mid z$$

Write $p = dk$ for some $k \in \mathbf{Z}[i]$. Since p is a Gaussian prime, one of u or k is unit in $\mathbf{Z}[i]$.
If k is unit, then $d = pk^{-1}$, and we see $p \mid d$ and $d \mid z$ which implies $p \mid z$, a contradiction. Thus, d is unit with $d^{-1} \in \mathbf{Z}[i]$. Now multiply $d = zs + pt$ by w to get

$$\begin{aligned} dw &= wzs + wpt \\ w &= d^{-1}wzs + d^{-1}wpt \\ w &= d^{-1}\ell ps + d^{-1}wpt \\ &= d^{-1}p(\ell s + pt) \end{aligned}$$

Thus, $p \mid w$.

We are now in a position to prove we have unique prime factorization in $\mathbf{Z}[i]$.

THEOREM 12.3

Every $z \in \mathbf{Z}[i]$, with $N(z) > 1$ has a unique factorization into primes (up to reordering and multiplication by units).

13 Congruences

Throughout this section, we fix a positive integer n, and call it a modulus. This comes from the Latin word for a "measure," or as we might say, a "yardstick." This modulus is used to compare two integers.

DEFINITION 13.1

Two integers a and b are said to be congruent modulo n, and we write

$$a \equiv b \pmod{n},$$

provided a and b have equal remainders between 0 and $n-1$ when they are each divided by n; that is, if

$$a = q_1 n + r_1 \text{ and } b = q_2 n + r_2,$$

where $0 \leq r_1, r_2 < n$, then $r_1 = r_2$.

When $n = 1$, we see that the only possible remainder upon division by 1 is 0. This is the trivial and interesting case. So, keep the story worthwhile, we typically assume that $n \geq 2$.

EXAMPLE 13.1

For instance, when the modulus is $n = 5$, here are all the integers congruent to each other with a remainder r ($0 \leq r < 5$) is of the form $5q + r$, where q is any integer.

- The integers with a remainder of 0:

$$\{5q : q \in \mathbf{Z}\} = \{0, \pm 5, \pm 10, \ldots\}.$$

- The integers with a remainder of 1:

$$\{5q + 1 : q \in \mathbf{Z}\} = \{\ldots, -9, -4, 1, 6, 11, \ldots\}.$$

- The integers with a remainder of 2:

$$\{5q + 2 : q \in \mathbf{Z}\} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}.$$

- The integers with a remainder of 3:

$$\{5q+3 : q \in \mathbf{Z}\} = \{\ldots, -7, -2, 3, 8, 13, \ldots\}.$$

- The integers with a remainder of 4:

$$\{5q+4 : q \in \mathbf{Z}\} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}.$$

The same observation applies to any modulus n. Given a modulus $n \geq 2$, the set of integers $\mathbf{Z}$ gets partitioned into n disjoint pieces according to the n possible remainders $0, 1, 2, \ldots, n-1$.

EXAMPLE 13.2

- We have $23 \equiv 37 \pmod 7$ since 23 and 37 both have a remainder of 2 when divided by 7.
- We have $12 \equiv 12 \pmod 5$ since 12 and 2 both have a remainder of 2 when divided by 5.

EXERCISE 13.1

Are the following statements true or false?

(1) $37 \equiv 13 \pmod 6$.

(2) $15 \equiv 15 \pmod 5$.

(3) $31 \equiv -4 \pmod 7$.

Solution:

(1) True.

(2) True.

(3) False.

EXERCISE 13.2

Find the smallest non-negative integer satisfying the congruence.

(1) $101 \equiv a \pmod 3$.

(2) $-7 \equiv a \pmod 5$.

(3) $45 \equiv a \pmod{11}$.

Solution:

(1) $a = 2$.

(2) $a = 3$.

(3) $a = 1$.

A rather surprising fact is that the congruence relation ($\equiv$) behaves much likely the equality relation ($=$).

PROPOSITION 13.1

The congruence relation ($\equiv$) is an equivalence relation ($=$); that is, it satisfies the following axioms:

(1) Reflexivity: If a is any integer, then $a \equiv a \pmod n$,

(2) *Symmetry: If* $a \equiv b \pmod{n}$*, then* $b \equiv a \pmod{n}$*,*

(3) *Transitivity: If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$*, then* $a \equiv c \pmod{n}$*.*

Proof: Exercise.

Here is a quick and alternate way to tell if $a \equiv b \pmod{n}$.

PROPOSITION 13.2

Two integers a *and* b *are congruent modulo* n *if and only if* $n \mid (a - b)$*.*

Proof: If $a \equiv b \pmod{n}$, then

$$a = q_1 n + r \text{ and } b = q_2 n + r,$$

for some integers q_1, q_2, and r, where $0 \leq r < n$. Then,

$$a - b = (q_1 - q_2)n,$$

which clearly shows that $n \mid (a - b)$.
On the other hand, suppose $n \mid (a - b)$ which implies $a - b = nk$ for some $k \in \mathbf{Z}$. According to Divison Algorithm, we have integers q, t, r, and s such that

$$a = nq + r,\ 0 \leq r < n \text{ and } b = nt + s,\ 0 \leq s < n.$$

Then,

$$\begin{aligned} r - s &= (a - nq) - (b - nt) \\ &= a - b + n(t - q) \\ &= nk + n(t - q) \\ &= n(k + t - q) \end{aligned}$$

So, $n \mid (r - s)$. If $r - s \neq 0$, then by Proposition 2.1(3) $n \leq |r - s|$. Since $0 \leq r < n$ where $0 \leq s < n$, we also have $|r - s|$ which contradicts $n < n$. This forces us to conclude that $r - s = 0$ implies $r = s$ and $a \equiv b \pmod{n}$.

Week 4 | Monday

23rd May

Victoria Day.

Lecture 10

25th May

PROPOSITION 13.3

Let $a, b, c, d \in \mathbf{Z}$*, and suppose that*

$$\begin{aligned} a &\equiv b \pmod{n}, \\ c &\equiv d \pmod{n}. \end{aligned}$$

Then,

$$\begin{aligned} a \pm c &\equiv b \pm d \pmod{n}, \\ ac &\equiv bd \pmod{n}. \end{aligned}$$

Proof: Use Proposition 2.1.

COROLLARY 13.1

Suppose $a, b, c \in \mathbf{Z}$, $n \geq 2$, and $a \equiv b \pmod{n}$, then

$$a \pm c \equiv b \pm d \pmod{n},$$
$$ac \equiv bd \pmod{n}.$$

COROLLARY 13.2

Let $a, b \in \mathbf{Z}$, $n \geq 2$, and $f(x)$ be a polynomial with integer coefficient. If $a \equiv b \pmod{n}$, then

$$f(a) = f(b) \pmod{n}.$$

EXAMPLE 13.3

Simplify $994 \cdot 996 \cdot 997 \cdot 998 \pmod{100}$ to a number in the range $\{0, 1, \ldots, 999\}$.

Solution: Rather than deal with large "positive" numbers, we'll convert them to small "negative" numbers:

$$994 \equiv -6 \pmod{1000}$$
$$996 \equiv -4 \pmod{1000}$$
$$997 \equiv -3 \pmod{1000}$$
$$998 \equiv -2 \pmod{1000}.$$

Therefore, $994 \cdot 996 \cdot 997 \cdot 998 \equiv (-6)(-4)(-3)(-2) \pmod{1000} \equiv 144 \pmod{1000}$.

EXAMPLE 13.4

Let $f(x) = x^5 - 10x + 7$. Compute the remainder of $f(27)$ divided by 5.

Solution: Note that $27 \equiv 2 \pmod{5}$, so

$$f(27) \equiv f(2) \pmod{5} \equiv 34 \pmod{5} \equiv 4 \pmod{5}.$$

Therefore, 4 is the remainder of $f(27)$ divided by 5.

PROPOSITION 13.4

Let $a \in \mathbf{Z}$ and $n \geq 2$. If $(a, n) = 1$, then there exists $b \in \mathbf{Z}$ such that $ab \equiv 1 \pmod{n}$.

If $(a, n) = 1$, then by Bezout's Identity, there exists $b, c \in \mathbf{Z}$ such that

$$ab + cn = 1.$$

By Proposition 13.2, $ab \equiv 1 \pmod{n}$.

DEFINITION 13.2

Let $a \in \mathbf{Z}$ and $n \in \mathbf{Z}^+$ such that $(a, n) = 1$. We call the integer b such that $ab \equiv 1 \pmod{n}$ the inverse of a modulo n and write

$$b \equiv a^{-1} \pmod{n}.$$

EXAMPLE 13.5

Find $47^{-1} \pmod{61}$.

Solution: Apply the Extended Euclidean Algorithm to 61 and 47:

r_i	q_{i-1}	s_i	t_i	Check
61		1	0	
47	1	0	1	
14	3	1	-1	$(1)(61) + (-1)(47) = 14$
5	2	-3	4	$(-3)(61) + (4)(47) = 5$
4	1	7	-9	$(7)(61) + (-9)(47) = 4$
1	4	-10	13	$(-10)(61) + (13)(47) = 1$

Write the linear combination, then reduce mod 61:

$$(-10) \cdot 61 + 13 \cdot 47 = 1$$
$$13 \cdot 47 \equiv 1 \pmod{61}.$$

Hence, $47^{-1} \equiv 13 \pmod{61}$.

COROLLARY 13.3

Let $a, b \in \mathbf{Z}$ and $n \in \mathbf{Z}$. If $(a, n) = 1$ and $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.

We can strengthen Corollary 13.3 further.

PROPOSITION 13.5

If $(a, n) = d$ and $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{\frac{n}{d}}$.

Proof: Proof. Suppose, $ab \equiv ac \pmod{n}$, then $n \mid ab - ac$ which implies there exists $k \in \mathbb{Z}$ such that

$$ab - ac = kn$$

Then,

$$(b - c)\frac{a}{d} = k\frac{n}{d}$$

Notice both $\frac{a}{d}$ and $\frac{n}{d}$ are integers because $(a, n) = d$. Since $\frac{a}{d}$ divides the RHS, it must divide the LHS, that is, $\frac{a}{d} \mid k\frac{n}{d}$. Further, by Proposition 4.2, $(\frac{a}{d}, \frac{n}{d}) = 1$, hence

$$\frac{a}{d} \mid k \qquad \text{by Proposition 6.2}$$
$$k = \frac{a}{d}\ell \qquad \text{for some } \ell \in \mathbb{Z}$$

Hence,

$$(b - c)\frac{a}{d} = \frac{a}{d}\ell\frac{n}{d},$$

which implies

$$b - c = l\frac{n}{d}$$

Thus,

$$b \equiv c \pmod{\frac{n}{d}}.$$

EXAMPLE 13.6

Reduce $5^{13} \pmod{17}$.

Solution: We have

$$\begin{aligned} 5^1 &\equiv 5 \pmod{17} \\ 5^2 &\equiv 25 \equiv 8 \pmod{17} \\ 5^4 &\equiv 64 \equiv -4 \pmod{17} \\ 5^8 &\equiv 16 \equiv -1 \pmod{17} \\ 5^{13} &\equiv (-1)(-4)(5) \equiv 3 \pmod{17}. \end{aligned}$$

EXERCISE 13.3

Find the remainder when 306^{100} is divided by 7.

Solution: TODO

In practice, in order to compute $a^k \pmod{n}$ for some large power n, we utilize the so-called Double-and-Add Algorithm. The algorithm is as follows: first write the integer k in its binary expansion, that is,

$$k = \sum_{i=0}^{t} c_i 2^i = c_t \cdot 2^t + c_{t-1} \cdot 2^{t-1} \cdots + c_1 \cdot 2 + c_0,$$

where $c_i \in \{0, 1\}$. Then,

$$\begin{aligned} a^k &\equiv a^{c_t \cdot 2^t + c_{t-1} \cdot 2^{t-1} \cdots + c_1 \cdot 2 + c_0} \\ &\equiv (a^{2^t})^{c_t} (a^{2^{t-1}})^{c_{t-1}} \cdots (a^2)^{c_1} (a^0)^{c_0} \pmod{n}. \end{aligned}$$

But then note that for j such that $2 \leq j \leq t$, we can deduce the value of a^{2^j} from $a^{2^{j-1}} \pmod{n}$ as follows:

$$a^{2^j} \equiv (a^{2^{j-1}})^2 \pmod{n}.$$

Therefore, we can compute $a^2, a^{2^2}, \ldots a^{2^t}$ in $t - 1$ steps.

EXAMPLE 13.7

Let us compute $n \equiv 7^{114} \pmod{23}$ such that $0 \leq n < 23$.

Solution: Note that

$$114 = 2^6 + 2^5 + 2^4 + 2 = 64 + 32 + 16 + 2.$$

Then,

$$\begin{aligned} 7^2 &\equiv 49 \equiv 3 \pmod{23} \\ 7^4 &\equiv (7^2)^2 \equiv 3^2 \equiv 9 \pmod{23} \\ 7^8 &\equiv (7^4)^2 \equiv 9^2 \equiv 81 \equiv 12 \pmod{23} \\ 7^{16} &\equiv (7^8)^2 \equiv 12^2 \equiv 144 \equiv 6 \pmod{23} \\ 7^{32} &\equiv (7^{16})^2 \equiv 6^2 \equiv 36 \equiv 13 \pmod{23} \\ 7^{64} &\equiv (7^{32})^2 \equiv 13^2 \equiv 169 \equiv 8 \pmod{23}. \end{aligned}$$

Thus,

$$\begin{aligned} 7^{114} &\equiv 7^{64+32+16+2} \pmod{23} \\ &\equiv 7^{64}7^{32}7^{16}7^{2} \pmod{23} \\ &\equiv (8)(13)(6)(3) \pmod{23} \\ &\equiv 1872 \pmod{23} \\ &\equiv 9 \pmod{23}. \end{aligned}$$

Lecture 11

27th May

We will now take a look at some interesting applications of modular arithmetic. For example, it can be used to demonstrate that certain Diophantine equations have no solutions.

EXAMPLE 13.8

Show that the Diophantine equation

$$x^2 + y^2 = 4z + 3$$

has no integer solutions x, y, z.

Solution: Since there are infinitely many possibilities for x, y, z, it seems a bit daunting to show that none of them work. But a little trick with congruences and replacement makes this problem quite straightforward. This is the same as solving the congruence

$$x^2 + y^2 \equiv 3 \pmod{4}$$

in integers x and y. Since every integer is congruent to either $0, 1, 2, 3$ modulo 4, there are essentially 16 possible combinations of x and y that we can check. However, the problem becomes even simpler if we note that

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 0,\ 3^2 \equiv 1 \pmod{4}.$$

Thus, every perfect square is congruent to either 0 or 1 modulo 4. Since we are dealing with the sum of two perfect squares, there are only three options left to check, namely

$$0 + 0 \equiv 0,\ 0 + 1 \equiv 1,\ 1 + 1 \equiv 2 \pmod{4}.$$

As we can see, none of them add up to 3, which implies that $x^2 + y^2 \equiv 3 \pmod{4}$ has no solution in integer x, y. Therefore, there are no solutions to the Diophantine equation $x^2 + y^2 = 4z + 3$.

EXAMPLE 13.9

Show that $x^5 \equiv x \pmod{5}$ for all $x \in \mathbf{Z}$.

Solution: Every integer x is congruent mod 5 to one of its possible remainders $0, 1, 2, 3, 4$. If the desired congruence holds for these remainders, then, by replacement, the congruence holds for any integer x. By routine calculation we see that

$$0^5 \equiv 0,\ 1^5 \equiv 1,\ 2^5 \equiv 2,\ 3^5 \equiv 3,\ 4^5 \equiv 4 \pmod{5}.$$

Having verified the result on the five possible remainders, replacement gives the result for all integers.

14 The Ring of Residue Classes $\mathbf{Z}_n$

Assume that the modulus n is a positive integer ($n \geq 2$). By the Division Algorithm, every integer b can be written as

$$b = qn + a,\ 0 \leq a < n.$$

Reducing this equation mod n, we have

$$b \equiv a \pmod{n}.$$

Since $0 \leq a < n$, we have $a \in \{0, 1, 2, \ldots, n-1\}$. In other words, mod n every integer can be reduced to a number in $\{0, 1, 2, \ldots, n-1\}$. This set is called the standard residue system mod n, and answers to modular arithmetic problems will usually be simplified to a number in this range.

DEFINITION 14.1

Let $a \in \mathbf{Z}$. The set

$$[a] = \{qn + a : q \in \mathbf{Z}\} = \{b \in \mathbf{Z} : b \equiv a \pmod{n}\}$$

is called the residue class (equivalence class of a modulo n). The integer a is called a representative of the residue class $[a]$. The finite set of residues mod n will be denoted $\mathbf{Z}_n$.

Remark: $[a] = [b] \iff b \equiv a \pmod{n}$.

EXAMPLE 14.1

For Example 3 (Lecture 9), the five residue classes of $\mathbf{Z}_n$ are:

$$[0] = \{0 + 5q : q \in \mathbf{Z}\}$$
$$[1] = \{1 + 5q : q \in \mathbf{Z}\}$$
$$[2] = \{2 + 5q : q \in \mathbf{Z}\}$$
$$[3] = \{3 + 5q : q \in \mathbf{Z}\}$$
$$[4] = \{4 + 5q : q \in \mathbf{Z}\}$$

EXERCISE 14.1

Let $n \in \mathbf{Z}^+$. Prove that the residue clases $[0], [1], \ldots, [n-1]$ modulo n partition $\mathbf{Z}$, that is,

$$[0] \cup [1] \cup \cdots \cup [n-1] = \mathbf{Z},$$

$[a] \cap [b] \neq \emptyset \implies [a] = [b]$.

PROPOSITION 14.1

Let $n \in \mathbf{Z}^+$ and consider the collection $\mathbf{Z}_n$ of all residues modulo n. Define the binary operation $+$, $-$, and $\cdot$ as follows:

$$[a] \pm [b] = [a \pm b],\ [a] \cdot [b] = [a \cdot b].$$

Then, under these binary operations, $\mathbf{Z}_n$ forms a commutative ring with identity $[1]$.

Proof: Use Proposition 1 (Lecture 10).

EXAMPLE 14.2

(a) What are the residue classes of modulo 6?

(b) Construct an addition table and multiplication table.

(c) Does the ring $\mathbf{Z}_6$ form an integral domain?

LECTURE 12
30th May

15 Linear Congruences

DEFINITION 15.1

An equation of the form

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k \equiv b \pmod{n}$$

with unknowns $x_1, x_2, \ldots, x_k$ is a linear congruence equation in k variables.

Observe that by definition of mod, we can rewrite a linear congruence equation as

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k - nx_{k+1} = b,$$

which is a Diophantine equation in $k+1$ variables.

Observe that a linear congruence equation either has no solution or infinitely many solutions. Indeed, if $x_i = s_i$, $1 \leq i \leq k$ is solutions of the form

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k \equiv b \pmod{n},$$

then

$$x_i = s_i + qn,\ 1 \leq i \leq k$$

is also a solution for all $q \in \mathbf{Z}$. This implies that the corresponding Diophantine equation also either has no solution or infinitely many solutions.

Remark: When writing the solutions of a linear congruence equation $ax \equiv b \pmod{n}$, we typically either write all solutions in the form

$$x \equiv s \pmod{n}$$

or we say that s is the unique solution modulo n.

THEOREM 15.1

Let $a, b \in \mathbf{Z}$ and $n \in \mathbf{Z}^+$. Let $(a, n) = d$ and consider the linear congruence

$$ax \equiv b \pmod{n}.$$

If $d \mid b$, then the linear congruence has no solution. If $d \mid b$, then the linear congruence has exactly d distinct solutions modulo n.

Proof: Solving the congruence $ax \equiv b \pmod{n}$ is equivalent to solving the linear Diophantine equation $ax + ny = b$ for some y. If $d \nmid b$, then the Diophantine equation has no solution, so the congruence has no solution either. If $d \mid b$, then by Theorem 1 (Lecture 5), the solution of the Diophantine equation take the form

$$x = x_0 - \frac{n}{d}t,\ y = y_0 + \frac{a}{d}t,$$

where (x_0, y_0) is any particular solution (obtained from the Euclidean algorithm, for instance).
We need to show that of these infinitely many solutions, there are exactly d distinct solutions mod n. Suppose two solutions of this form are congruent mod n, that is,

$$x_0 - \frac{n}{d}t_1 \equiv x_0 - \frac{n}{d}t_2 \pmod{n}.$$

Then,

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}.$$

Now, $\left(\frac{n}{d}, n\right) = \frac{n}{d}$, so by Proposition 3 (Lecture 10), we can divide this congruence by $\frac{n}{d}$ to obtain

$$t_1 \equiv t_2 \pmod{d}.$$

Likewise, suppose $t_1 \equiv t_2 \pmod{d}$. This means that t_1 and t_2 differ by a multiple of d, that is,

$$t_1 - t_2 = kd.$$

So,

$$\frac{n}{d}t_1 - \frac{n}{d}t_2 = \frac{n}{d}kd = nk.$$

This implies that

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}.$$

By Corollary 1 (Lecture 10),

$$x_0 - \frac{n}{d}t_1 \equiv x_0 - \frac{n}{d}t_2 \pmod{n}.$$

We have proven that two solutions of the above form are equal mod n if and only if their parameter values are equal mod d, that is, If we let t range over a complete system of residues mod d, then $x_0 + \frac{n}{d}t$ ranges over all possible solutions mod n. To be very specific, all the solutions mod n are given by

$$x_0 + \frac{n}{d}t \pmod{n},\ t = 0, 1, 2, \ldots, d-1.$$

COROLLARY 15.1

Let $a, b \in \mathbf{Z}$ and $n \in \mathbf{Z}^+$. If $(a, n) = 1$, then the equation

$$ax \equiv b \pmod{n}$$

has a solution. Moreover, the unique solution modulo n is

$$x \equiv a^{-1}b \pmod{n}.$$

EXAMPLE 15.1

Solve $6x \equiv 7 \pmod{8}$.

Solution: Since $(6, 8) = 2 \mid 7$, there are no solutions.

EXAMPLE 15.2

Solve $3x \equiv 7 \pmod{4}$.

Solution: Since $(3, 4) = 1 \mid 7$, there is exactly one solution modulo 7. We have $3x + 4y = 7$ for some $y \in \mathbf{Z}$. By the EEA, we have

r_i	q_{i-1}	s_i	t_i	Check
4		1	0	
3	1	0	1	
1	3	1	-1	$4 \cdot 1 + 3 \cdot (-1) = 1$

So, $4 \cdot 7 + 3 \cdot (-7) = 7$. Thus, $x_0 = -7$, $y_0 = 7$ is a particular solution. So the general solution is:

$$x = -7 - 4t,\ y = 7 + 3t.$$

The y equation is irrelevant, and the x equation says

$$x \equiv 1 \pmod 4.$$

EXAMPLE 15.3

Find all solutions of $7x \equiv 5 \pmod{39}$.

Solution: Since $(7, 5) = 1 \mid 39$, there is exactly one solution modulo 39. We have $7x + 39y = 5$ for some $y \in \mathbf{Z}$. By the EEA, we have

r_i	q_{i-1}	s_i	t_i	Check
39		1	0	
7	5	0	1	
4	1	1	-5	$39(1) + 7(-5) = 4$
3	1	-1	6	$39(-1) + 7(6) = 3$
1	3	2	-11	$39(2) + 7(-11) = 1$

So,

$$\begin{aligned} 7(-11) + 39(2) &= 1 \\ 7(-11 \cdot 5) + 39(2 \cdot 5) &= 1 \cdot 5 \\ 7(-55) + 39(10) &= 5. \end{aligned}$$

Thus, $x_0 = -55$, $y_0 = 10$ is a particular solution. The general solution is:

$$x \equiv x_0 + \frac{n}{d}(0) \equiv -55 \equiv 23 \pmod{39}.$$

16 Linear Equations in $\mathbf{Z}_n$

Let n be a modulus. We will now turn our attention to equations in $\mathbf{Z}_n$. Let $a, b \in \mathbf{Z}$, and consider

$$[a][x] = [b]$$

in $\mathbf{Z}_n$ where $x \in \mathbf{Z}$ is unknown.

EXAMPLE 16.1

The linear equation $[2][x] = [3]$ has only one solution in $\mathbf{Z}_9$, namely $[x] = [6]$.

EXAMPLE 16.2

The equation $[3][x] = [7]$ has no solution in $\mathbf{Z}_9$.

EXAMPLE 16.3

The linear equation $[3][x] = [6]$ has three solutions in $\mathbf{Z}_9$, namely $[x] = [2]$, $[x] = [5]$, and $[x] = [8]$.

Note: From Example 6, we see the principal difference between the linear equations in $\mathbf{Z}_n$ and the linear equation $cx = d$ in $\mathbf{Z}$. The only way $cx = d$ can have more than one solution is if $c = d = 0$.

It turns out that the tools that we have in our hands right now can help us to solve the linear congruence easily. Observe that

$$\begin{aligned}[a][x] &= [b] \\ [ax] &= [b],\end{aligned}$$

and this is the same as solving the linear congruence

$$ax \equiv b \pmod{n}.$$

PROPOSITION 16.1

Let $a, b \in \mathbf{Z}$, $n \in \mathbf{Z}^+$ and $a \neq 0$. The linear equation $[a][x] = [b]$ in $\mathbf{Z}_n$ if $d = (a, n) \mid b$ and total no. of residue classes satisfying $[a][x] = [b]$ in $\mathbf{Z}_n$ is equal to $d = (a, n)$.

EXAMPLE 16.4

Solve $[440][x] = [80]$ in $\mathbf{Z}_{300}$.

Solution: By the EEA, the general solution to $440x + 300y = 80$ is

$$x = -8 - 15t,\ y = 12 + 22t,\ t \in \mathbf{Z}.$$

By evaluating $-8 - 15t$ at $t = 0, 1, \ldots, 19$, we obtain 20 distinct solutions in $\mathbf{Z}_{300}$.

PROPOSITION 16.2

Let $a, b \in \mathbf{Z}$, $n \in \mathbf{Z}^+$, and $(a, n) = 1$. The linear equation $[a][x] = [b]$ has a unique solution in $\mathbf{Z}_n$.

17 Chinese Remainder Theorem

Around the year 300 a solution to the following mathematical problem appeared in the mathematical manual of Chinese Master, Sun Tzu Suan Ching.

"We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?"

The master was asking us to solve the three simultaneous congruences:

$$\begin{aligned}x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7}.\end{aligned}$$

The Chinese remainder theorem tells us that $x \equiv 23 \pmod{105}$ is the solution to above problem.

Before proceeding to its statement, let us prove the following result.

PROPOSITION 17.1

Let m and n be integers greater than 1 that are coprime (relatively prime). Then the congruence

$$a \equiv b \pmod{mn}$$

is true if and only if both the congruences

$$\begin{aligned}a &\equiv b \pmod{m} \\ a &\equiv b \pmod{n}\end{aligned}$$

are true.

Proof: Suppose that $a \equiv b \pmod{mn}$, then $mn \mid (a-b)$, so $m \mid (a-b)$ and $n \mid (a-n)$. Therefore, $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. On the other hand, suppose that $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, Then, $m \mid (a-b)$ and $n \mid (a-b)$. Since $(m,n) = 1$, $mn \mid (a-b)$ by Proposition 1 (Lecture 4). Thus, $a \equiv b \pmod{mn}$.

THEOREM 17.1: The Chinese Remainder Theorem (CRT)

If m, n are coprime (relatively prime) moduli and $a, b \in \mathbf{Z}$, then

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

have a common solution x_0. Furthermore, any two solutions x_0, y_0 to this pair of congruences must be such that $x_0 \equiv y_0 \pmod{mn}$. The congruences have a unique solution.

Proof: Since m, n are coprime, by Bezout's Identity there exists $x, y \in \mathbf{Z}$ such that

$$mx + ny = 1.$$

Multiplying both sides by $(b-a)$, we obtain a solution to

$$mx' + ny' = b - a,$$

where $x' = (b-a)x$ and $y' = (b-a)y$. Thus, $a + mx' = b - ny' = x_0$, we see that

$$x_0 \equiv a \pmod{m}$$
$$x_0 \equiv b \pmod{n}.$$

So x_0 is a common solution. Now, let y_0 be any other solution to the system of congruences, then

$$x_0 \equiv y_0 \pmod{m}$$
$$x_0 \equiv y_0 \pmod{n}.$$

So, by Proposition 3, we conclude that

$$x_0 \equiv y_0 \pmod{mn}.$$

Lecture 13
1st June

Here is an alternate proof for Chinese Remainder Theorem.

We have that there exists $s \in \mathbf{Z}$ such that $x = ms + a$. Substituting this into the other congruence gives

$$ms + a \equiv b \pmod{n}$$
$$ms \equiv (b-a) \pmod{n}.$$

Since $(m,n) = 1$, there exists $c \in \mathbf{Z}$ such that $ms \equiv 1 \pmod{n}$. Multiplying by c gives

$$s \equiv c(b-a) \pmod{n}.$$

Thus, there exists $t \in \mathbf{Z}$ such that $s = tn + c(b-a)$.

Hence,

$$x = m\big(tn + c(b-a)\big) + a$$
$$= mnt + mc(b-a) + a.$$

Thus, the unique solution is

$$x \equiv mc(b-a) + a \pmod{mn}.$$

We can easily generalize this result to arbitrary number of coprime moduli.

THEOREM 17.2: Generalized Chinese Remainder Theorem

Suppose $n_1, \ldots, n_k$ are moduli that are pairwise coprime. If $a_1, \ldots, a_k \in \mathbf{Z}$ then there exists $x \in \mathbf{Z}$ such that

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ &\vdots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

Furthermore, if x_0 is a solution of these congruences, then the complete solution to all the equations is given by all

$$x \equiv x_0 \pmod{n_1 \cdots n_k}.$$

Process to solve systems of congruences with CRT:

- Begin with the largest modulus $x \equiv a_k \pmod{n_k}$. Rewrite it as $x = n_k j_k + a_k$ for some $j_k \in \mathbf{Z}$.
- Substitute the expression for x into the congruence with the next largest modulus, that is,

$$x \equiv a_{k-1} \pmod{n_{k-1}} \implies n_k j_k + a_k \equiv a_{k-1} \pmod{n_{k-1}}.$$

- Solve this congruence for j_k.
- Write the solved congruence as an equation, and then substitute this expression for j_k into the equation for x.
- Continue substituting and solving the congruences until the equation for x implies the solution to the system of congruences.

EXAMPLE 17.1

Solve the system of congruences:

$$\begin{aligned} x &\equiv 3 \pmod{6} \\ x &\equiv 7 \pmod{13}. \end{aligned}$$

Solution: First, $x \equiv 7 \pmod{13} \iff x = 13j + 7$ for some $j \in \mathbf{Z}$. Then,

$$x \equiv 3 \pmod{6} \implies 13j + 7 \equiv 3 \pmod{6}.$$

Now, solve for j to get: $j \equiv 2 \pmod{6} \iff j = 6k + 2$ for some $k \in \mathbf{Z}$. Then,

$$x = 13(6k+2) + 7 = 78k + 33 \implies x \equiv 33 \pmod{78}.$$

EXERCISE 17.1

Solve the system of congruences:

$$\begin{aligned} x &\equiv 6 \pmod{11} \\ x &\equiv 13 \pmod{16} \\ x &\equiv 9 \pmod{21} \end{aligned}$$

EXERCISE 17.2

Calvin Butterball keeps pet meerkats in his backyard. If he divides them into 5 equal groups, 4 are left over. If he divides them into 8 equal groups, 6 are left over. If he divides them into 9 equal groups, 8 are left over. What is the smallest number of meerkats that Calvin could have?

Sometimes we can solve a system even if moduli aren't relatively prime.

THEOREM 17.3

Consider the system of congruences:

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}.$$

(a) If $(m, n) \nmid (a - b)$, then there are no solutions.

(b) If $(m, n) \mid (a - b)$, then there is a unique solution mod $[m, n]$.

Proof: Exercise.

18 Euler φ Function and Euler's Theorem

Firstly, we will study the units for $\mathbf{Z}_n$.

DEFINITION 18.1

Let $n \geq 2$. An element $[a]$ in $\mathbf{Z}_n$ is a unit provided the equation $[a][x] = [1]$ has a unique solution. The integer a representing $[a]$ is then called unit modulo n. The unique $[x]$ is called the inverse of $[a]$ in $\mathbf{Z}_n$. The set of all units of $\mathbf{Z}_n$ is denoted by $\mathbf{Z}_n^*$.

Remark: Proposition 2 (Lecture 12) tells the ways to think about units. An element $[a] \in \mathbf{Z}_n$ is unit if and only if a is coprime with n.

PROPOSITION 18.1

If p is a prime and $[a] \neq 0$ in $\mathbf{Z}_p$, then $[a]$ is a unit. In other words, every non-zero element of $\mathbf{Z}_p$ is a unit.

The importance of Proposition 1 lies in the fact that $\mathbf{Z}_p$ behaves just like the well understood sets of numbers $\mathbf{Q}, \mathbf{R}, \mathbf{C}$. Namely, $\mathbf{Z}_p$ admits addition, subtraction, multiplication, and division by everything except zero. Indeed, if $[a] \neq 0$ in $\mathbf{Z}_p$, then $[a][x] = [b]$ always has a solution. So we can divide. Systems that admits all four of the arithmetic operation are usually called **fields**.

PROPOSITION 18.2

Let $n \geq 2$. Then,

i. The product of a unit is another unit, that is, if $[a], [b] \in \mathbf{Z}_n^*$, then $[a][b] \in \mathbf{Z}_n^*$.

ii. The product of units is associative, that is, $([a][b])[c] = [a]([b][c])$ for all $[a], [b], [c]\mathbf{Z}_n^*$.

iii. The residue class $[1]$ is always a unit, that is, $[1] \in \mathbf{Z}_n^*$.

iv. The inverse of a unit is also a unit, that is, if $a \in \mathbf{Z}_n^*$ and $x \in \mathbf{Z}_n^*$ is a unique residue class that gives $[a][x] = [1]$, then $[x] \in \mathbf{Z}_n^*$. The product of units is commutative, that is, $[a][b] = [b][a]$ in $\mathbf{Z}_n^*$.

Any set that enjoys the five properties of Proposition 2 is called an Abelian Group.

EXAMPLE 18.1

Compute $\mathbf{Z}_{10}^*$ and construct its multiplication table.

Solution: The integers that are coprime to 10 are 1, 3, 7, and 9. Thus, $\mathbf{Z}_{10}^* = \{[1], [3], [7], [9]\}$ and its multiplication table is TODO.

Lecture 14

3rd June

As you may have noticed already, the condition that numbers are relatively prime is useful and interesting. So, it should not be surprising that there are times when it is useful to restrict a complete residue system modulo n to just the numbers which are relatively prime to n.

DEFINITION 18.2

Let $\varphi(n)$ denote the number of integers m such that $0 \leq m < n$ and $(m, n) = 1$. The function φ is called the Euler's totient function.

EXAMPLE 18.2

Find $\varphi(18)$.

Solution: Numbers from 0 to 17 that are coprime with 18 are $1, 5, 7, 11, 13, 17$. So, $\varphi(18) = 6$.

EXAMPLE 18.3

Find $\varphi(101)$.

Solution: Since 101 is itself prime, the full list of numbers that are coprime with 101 are $1, 2, 3, \ldots, 100$. Thus, $\varphi(101) = 100$.

Remark: For any prime p, the numbers $1, 2, \ldots, (p-1)$ are coprime with p. Therefore, $\varphi(p) = p - 1$.

THEOREM 18.1: Euler's Theorem

If $[a] \in \mathbf{Z}_n^*$, *then* $[a]^{\varphi(n)} = [1]$.

Proof: Let $k = \varphi(n)$. Let $[u_1], \ldots, [u_k]$ be the complete list of residues of $\mathbf{Z}_n^*$. Form a new list

$$[a][u_1], \ldots, [a][u_k].$$

Since $\mathbf{Z}_n^*$ is a group, this list of residues is also in $\mathbf{Z}_n^*$. Furthermore, no element appears in this list twice, so if $[a][u_i] = [a][u_j]$ for some $i \neq j$, then $[u_i] = [u_j]$ by cancelling the unit $[a]$. Hence, the second list is a permutation of the original list.
It follows that the product of residues in the first list equals to the product of residues in the second list. After all, the two lists contain the same residues, only written in a different order. Thus, we obtain

$$[u_1][u_2] \cdots [u_k] = ([a][u_1]) \cdots ([a][u_k]).$$

Now, we can cancel the unit element $[u_1] \cdots [u_k]$ and conclude that $[a]^{\varphi(n)} = [1]$.

In the language of congruences, Euler's Theorem translates to

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

for any integer that is invertible modulo n, that is, $(a, n) = 1$. In other words, if a is coprime with modulus n, then

$$\frac{a^{\varphi(n)} - 1}{n} \in \mathbf{Z}.$$

EXAMPLE 18.4

Prove $623^{1222} \equiv 1 \pmod{1223}$.

Solution: $\varphi(1223) = 1222$ and $(1223, 623) = 1$. Hence, by Euler's Theorem $623^{1222} \equiv 1 \pmod{1223}$.

When the modulus is a prime, say p, we know that $\varphi(p) = p - 1$. Thus, Euler's Theorem specializes to another famous result attributed by Fermat.

THEOREM 18.2: Fermat's Little Theorem

If p is a prime and $p \nmid a$ for $p \in \mathbf{Z}_n^*$, then

$$[a]^{p-1} = [1].$$

In other words,

$$a^{p-1} \equiv 1 \pmod{p}.$$

COROLLARY 18.1: Fermat Variant

If p is a prime and $a \in \mathbf{Z}$, then

$$a^p = a \pmod{p}.$$

Proof: If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Theorem. Multiplying by a to get $a^p \equiv a \pmod{p}$. On the other hand, if $p \mid a$, then $a \equiv 0 \pmod{p}$, in which case it is obvious that

$$a^p \equiv 0^p \equiv 0 \equiv a \pmod{p}.$$

So the result holds for all $a \in \mathbf{Z}$.

19 Pseudoprimes

The converse of Fermat's Little Theorem is not true in general, that is, if there exists a such that $a^{n-1} \equiv 1 \pmod{n}$, then we can not infer that n is prime.

DEFINITION 19.1

A number n that is composite and satisfies $a^{n-1} \equiv 1 \pmod{n}$ is called a Fermat pseudoprime to base a. In the special case of $a = 2$, it is sometimes called the **Poulet number**.

EXAMPLE 19.1

The following table gives us the first Fermat pseudoprime to some small bases a:

a	Fermat pseudoprime
2	$341, 561, 645, 1105, 1387, 1729, 1905$
3	$91, 121, 286, 671, 703, 949, 1105, 1541, 1729$
4	$15, 85, 91, 341, 435, 561, 645, 703$
5	$4, 124, 217, 561, 781, 1541, 1729, 1891$

The first example of even pseudoprime ($n = 161038$) to the base 2 was given by Lehmer in 1950.

EXAMPLE 19.2

Prove that 341 is a Fermat pseudoprime to the base 2.

Solution: We want to show that $2^{340} \equiv 1 \pmod{341}$. Note that $341 = 11 \times 31$. By FLT, $2^{10} \equiv 1 \pmod{11}$. Thus,

$$2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{11}.$$

Thus, $11 \mid (2^{340} - 1)$. Also, $2^5 \equiv 32 \equiv 1 \pmod{31}$. So,

$$2^{340} \equiv (2^5)^{68} \equiv 1 \pmod{31}.$$

Thus, $31 \mid (2^{340} - 1)$. So, by Proposition 1 (Lecture 4), $341 \mid (2^{340} - 1)$.

EXERCISE 19.1

Show that 341 is not a Fermat pseudoprime.

Solution: We want to show that $3^{340} \not\equiv 1 \pmod{341}$. Note that $341 = 11 \times 31$. By FLT, $3^{10} \equiv 1 \pmod{11}$. Thus, $3^{340} = (3^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{11}$. So we need to show that $3^{340} \not\equiv 1 \pmod{31}$. Note that $340 = 30 \times 11 + 10$ and by FLT $3^{30} \equiv 1 \pmod{31}$.

$$3^{340} \equiv (3^{11})^{30} 3^{10} \equiv 1^{30} 3^{10} \equiv 3^{10} \pmod{31}.$$

So, $3^2 \equiv 9 \pmod{31}$, $3^3 \equiv 27 \equiv -4 \pmod{31}$, $3^4 \equiv 81 \equiv 19 \pmod{31}$, $3^6 \equiv (3^3)^2 \equiv (-4)^2 \equiv 16 \pmod{31}$. Therefore,

$$3^{10} \equiv 3^6 \cdot 3^4 \equiv 16 \cdot 19 \equiv 304 \pmod{31} \equiv 25 \pmod{31}.$$

Note that $3^{340} \equiv 25 \not\equiv 1 \pmod{31}$.

20 Polynomial Congruence

We have seen how to solve linear congruences $ax \equiv b \pmod{n}$. What about polynomial congruences? These, of course, are also important in number theory.

We first note that there are some immediate differences from what we are used to with solving polynomials over $\mathbf{R}$.

For example, we know the polynomial $f(x) = x^2 + 1$ has no roots over $\mathbf{R}$, but

$$x^2 + 1 \equiv 0 \pmod{5}$$

has $x = 2$ and $x = 3$ as solutions.

Also, we are used to d^{th} degree polynomials having exactly d roots, but

$$x^2 + x \equiv 0 \pmod{6}$$

has four distinct roots modulo 6, namely $x = 0, 2, 3, 5$.

The Chinese Remainder Theorem can also be utilized to solve polynomial congruences.

DEFINITION 20.1

Let d be a positive integer and consider a polynomial

$$f(x) = c_d x^d + \cdots + c_1 x + c_0,$$

where $c_0, \ldots, c_d \in \mathbf{Z}$ and $c_d \neq 0$. Then the congruence of the form $f(x) \equiv 0 \pmod{n}$ is called a

polynomial congruence.

Goal: Find all $x \in \mathbf{Z}$ which satisfy the above congruence.

Note that if we replace c_i with $[c_i]$, then we reduce the polynomial from $\mathbf{Z}$ to $\mathbf{Z}_n$. Solving the above congruence is equivalent to solving $f([x]) = [0]$ in $\mathbf{Z}_n$. If such an equation is satisfied by some residue class $[x_0]$, we say that $[x_0]$ is a root of $f(x)$ in $\mathbf{Z}_n$.

LECTURE 15

6th June

THEOREM 20.1

If $f(x)$ is a polynomial with integer coefficients and $f(a) \equiv 0 \pmod{n}$, then there exists a polynomial $g(x)$ with integer coefficients such that $f(x) \equiv (x-a)g(x) \pmod{n}$.

Proof: Using Polynomial division, we can divide $f(x)$ by $(x-a)$ to get

$$f(x) = (x-a)g(x) + b,\ b \in \mathbf{Z}.$$

Substitute a to get $f(a) = b$. Thus,

$$b \equiv f(a) \equiv 0 \pmod{n}.$$

Hence, $f(x) \equiv (x-a)g(x) \pmod{n}$.

EXAMPLE 20.1

Factor $f(x) = x^2 + 1 \pmod{5}$.

Solution: We saw that $x = 2$ is a root of $f(x)$ modulo 5. Using long division, we have $x^2 + 1 = (x-2)(x+2) \pmod{5}$. Alternatively, observe that

$$x^2 + 1 \equiv x^2 - 4 \equiv (x-2)(x+2) \pmod{5}.$$

PROPOSITION 20.1

Let $f(x)$ be a polynomial with integer coefficients. Let m and n be coprime moduli.

$$f(x) \equiv 0 \pmod{mn} \iff f(x) \equiv 0 \pmod{m} \wedge f(x) \equiv 0 \pmod{m}.$$

Proof: Similar to the proof of Proposition 3 (Lecture 12).

If $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of n, and $x_1, \ldots, x_k \in \mathbf{Z}$ satisfy

$$f(x_i) \equiv 0 \pmod{p_i^{e_i}},\ i = 1, \ldots, k,$$

then we can find x such that $x \equiv x_i \pmod{p_i^{e_i}}$ for all i using the GCRT, but then such an x would satisfy $f(x) \equiv 0 \pmod{p_i^{e_i}}$ for all i, and so $f(x) \equiv 0 \pmod{n}$. It follows that if each congruence $f(x) \equiv 0 \pmod{p_i^{s_i}}$ has a solution s_i, then $f(x) \equiv 0 \pmod{n}$ has $s_1 \cdots s_k$ solutions by the GCRT.

Now, we would show that a polynomial congruence $f(x) \equiv 0 \pmod{p}$ has at most d solutions, where d is the degree of $f(x)$.

PROPOSITION 20.2: Lagrange's Theorem

If p is a prime and $f(x)$ is a non-zero polynomial of degree d modulo p, then $f(x) \equiv 0 \pmod{p}$ has at most d distinct roots modulo p.

Proof: Omitted.

EXAMPLE 20.2

Solve the polynomial congruence:

$$x^{49} + 2x^{33} + 24 \equiv 0 \pmod{119}.$$

Solution: Note that $119 = 7 \times 17$. So by Proposition 1, there is a one-to-one correspondence between the roots of the above congruence and the roots to the system of congruences

$$\begin{aligned} x^{49} + 2x^{33} + 24 &\equiv 0 \pmod{7} \\ x^{49} + 2x^{33} + 24 &\equiv 0 \pmod{17}. \end{aligned}$$

Consider $n = 7$ with $\varphi(7) = 6$. Note that $x \equiv 0 \pmod{7}$ is not a solution. This means that $(x, 7) = 1$, so by Euler's Theorem

$$\begin{aligned} x^{49} + 2x^{33} + 24 &\equiv x^{8\cdot 6+1} + 2x^{5\cdot 6+3} + 24 \\ &\equiv x + 2x^3 + 24 \\ &\equiv 2x^3 + x + 24 \pmod{7}. \end{aligned}$$

After evaluating the LHS at $x = 1, \ldots, 6$, we see that the only solutions are

$$x \equiv 2 \pmod{7}, \ x \equiv 6 \pmod{7}.$$

Consider $n = 17$ with $\varphi(17) = 16$. Note that $x \equiv 0 \pmod{17}$ is not a solution. This means that $(x, 17) = 1$, so by Euler's Theorem

$$\begin{aligned} x^{49} + 2x^{33} + 24 &\equiv x^{3\cdot 16+1} + 2x^{2\cdot 16+1} + 24 \\ &\equiv x + 2x + 24 \\ &\equiv 3x + 24 \pmod{17}. \end{aligned}$$

Thus, we need to solve the congruence

$$\begin{aligned} 3x + 24 &\equiv 0 \pmod{17} \\ 3x &\equiv 10 \pmod{17} \\ 6 \cdot 3x &\equiv 6 \cdot 10 \\ x &\equiv 9 \pmod{17}. \end{aligned}$$

By Theorem 1 (Lecture 12), this is the only solution. Since there are two solutions modulo 7 and only one solution modulo 17, we conclude that there are $2 \cdot 1$ solutions modulo 119. These solutions correspond to two system of equations

$$\begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 9 \pmod{17}, \end{cases} \qquad \begin{cases} x \equiv 6 \pmod{7} \\ x \equiv 9 \pmod{17}. \end{cases}$$

$$\begin{aligned} x \equiv 2 \pmod{17} \iff x = 7j + 2 &\equiv 9 \pmod{17} \\ 7j &\equiv 7 \pmod{17} \\ j \equiv 1 \pmod{17} \iff j &= 17k + 1. \end{aligned}$$

So $x = 7(17k + 1) + 2 = 119k + 9$. Therefore, $x \equiv 9 \pmod{119}$ is a solution to the first system. The second system of congruences can be solved analogously and gives us a solution $x \equiv 111 \pmod{119}$.

EXERCISE 20.1

Find all the roots of $f(x) = x^3 + 3x^2 + 31x + 23$ modulo 35.

EXERCISE 20.2

Find all solutions of $f(x) = x^2 + x$ modulo 6.

EXAMPLE 20.3

Note that $2x - 4 \equiv 0 \pmod 6$ has two roots, namely

$$x \equiv 2 \pmod 6, \quad x \equiv 5 \pmod 6.$$

But the degree of the polynomial is 1.

LECTURE 16
8th June

21 The Order of Elements in $\mathbf{Z}_n^*$

Let n be a modulus. We already looked at certain kinds of equations in $\mathbf{Z}_n$. For example, in Lecture 11, we learned that neither $[x]^2 + [y]^2 = 3$ in $\mathbf{Z}_4$ nor $[x]^2 + [y]^2 + [z]^2 = 7$ in $\mathbf{Z}_8$ have solutions. In Lecture 12, we studied the equation $[a][x] = [b]$ in $\mathbf{Z}_n$ and saw that the usual application of the Extended Euclidean Algorithm allows us to produce all of its solutions.

Now, we want to understand how to handle *exponential* equations in $\mathbf{Z}_n^*$. In these kinds of equations, we are given residue classes $[a]$ and $[b]$ from $\mathbf{Z}_n^*$, and we want to determine all integer solutions x to the equation $[a]^x = [b]$. This is essentially the same as solving the congruence

$$a^x \equiv b \pmod n.$$

The problem of finding solutions to these exponential equations is known as the *discrete logarithm problem*, or DLP.

EXAMPLE 21.1

We already saw an example of an exponential equation in $\mathbf{Z}_n^*$, namely

$$a^x \equiv 1 \pmod n.$$

According to Euler's Theorem, this equation always has a non-zero solution whenever a and n are coprime. In particular, any $x \equiv 0 \pmod{\varphi(n)}$ satisfies the above congruence, for if $x \equiv \varphi(n)k$ for some integer k, then

$$a^x \equiv a^{\varphi(n)k} \equiv (a^{\varphi(n)})^k \equiv 1^k \equiv 1 \pmod n.$$

However, we do not know whether there are no other solutions to this equation. Depending on the choice of a, there might exist other solutions as well.

In order to understand how solutions to $a^x \equiv b \pmod n$ look like, we need to understand certain fundamental properties of group units in $\mathbf{Z}_n^*$.

DEFINITION 21.1

If $a \in \mathbf{Z}_n^*$, the **order** of a is the smallest exponent $k \geq 1$ such that $[a]^k = 1$. The order is denoted by $k = \operatorname{ord}(a)$.

EXAMPLE 21.2

The order of $[5]$ in $\mathbf{Z}_{13}^*$ is 4. Indeed, $[5]^4 = [1]$.

From Euler's Theorem, it follows that for all $a \in \mathbf{Z}_n^*$, it is the case that $\text{ord}(a) \leq \varphi(n)$. In fact, a much stronger result holds.

PROPOSITION 21.1

Let $a \in \mathbf{Z}$, $n \geq 2$, and $(a, n) = 1$. A positive integer m satisfies $a^m \equiv 1 \pmod{n}$ if and only if $\text{ord}(a) \mid m$.

Proof: By the Division Algorithm, we have

$$m = kq + r \text{ where } 0 \leq r < k.$$

Then, since $a^k \equiv 1 \pmod{n}$, we obtain

$$1 \equiv a^m \equiv a^{kq+r} \equiv (a^k)^q a^r \equiv 1^q a^r \equiv a^r \pmod{n}.$$

Since k is the order of a congruence modulo n, it must be the case $r = 0$. Hence, $k \mid m$.
On the other hand, let $m = kq$ for some q. Then,

$$a^m \equiv a^{kq} \equiv (a^k)^q \equiv 1^q \equiv 1 \pmod{n}.$$

COROLLARY 21.1

If $a \in \mathbf{Z}$, $n \geq 2$, and $(a, n) = 1$, then $\text{ord}(a) \mid \varphi(n)$.

Proof: By Euler's Theorem, $a^{\varphi(n)} \equiv 1 \pmod{n}$. So by Proposition 1, we have $\text{ord}(a) \mid \varphi(n)$.

Let D be the set of positive divisors of $\varphi(n)$. By Corollary 1, to find order of an $a \in \mathbf{Z}$ modulo n, we just need to find the smallest element of D such that $a^d \equiv 1 \pmod{n}$. Thus, the result greatly narrows down which powers we have to check.

EXAMPLE 21.3

Find the order of 3 and 9 modulo 17.

Solution: For $n = 17$, $\varphi(17) = 16$. The complete list of positive divisors of 16 are $D = \{1, 2, 4, 8, 16\}$. The smallest d satisfying $3^d \equiv 1 \pmod{17}$ is the order of 3 modulo 17. Thus,

$$\begin{aligned} 3^1 &\equiv 3 \pmod{17} \\ 3^2 &\equiv 9 \pmod{17} \\ 3^4 &\equiv 9^2 \equiv 81 \equiv -4 \pmod{17} \\ 3^8 &\equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17} \\ 3^{16} &\equiv (-1)^2 \equiv 1 \pmod{17}. \end{aligned}$$

Thus, $\text{ord}(3) = 16$.
For order of 9,

$$\begin{aligned} 9^1 &\equiv 9 \pmod{17} \\ 9^2 &\equiv 81 \equiv -4 \pmod{17} \\ 9^4 &\equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17} 9^8 \qquad \equiv (-1)^2 \equiv 1 \pmod{17}. \end{aligned}$$

Thus, $\text{ord}(9) = 8$.

EXERCISE 21.1

Can we find the order of 4 in modulo 6? Find the order of 5 in modulo 6.

Proposition 1 allows us to clarify all solutions to the exponential congruence

$$a^x \equiv b \pmod{n} \text{ where } (a,n) = 1 = (b,n).$$

PROPOSITION 21.2

Let $a, b \in \mathbf{Z}$, $n \in \mathbf{Z}^+$, and $(a,n) = 1 = (b,n)$. If x is a solution to the congruence $a^x \equiv b \pmod{n}$, then all solutions x' satisfy

$$x \equiv x' \pmod{\varphi(n)}.$$

Proof: Let x be a solution to $a^x \equiv b \pmod{n}$, and let $k = \text{ord}(a)$. By the Division Algorithm, we have

$$x = kq + r \text{ where } 0 \leq r < k.$$

But then,

$$a^x \equiv a^{kq+r} \equiv (a^k)^q a^r \equiv 1^q a^r \equiv a^r \pmod{n}.$$

Thus, WLOG we may assume $0 \leq x < k$.
Now, suppose there exists some other x' such that $a^{x'} \equiv b \pmod{n}$. Once again, WLOG, we may assume that $0 \leq x \leq x' < k$. But then,

$$a^x \equiv b \equiv a^{x'} \pmod{n} \implies a^{x'-x} \equiv 1 \pmod{n},$$

since $0 \leq x' - x < k$ and k is the order of a. So, we have $x' - x = 0$. Therefore, all solutions x' to $a^x \equiv b \pmod{n}$ satisfy $x' \equiv x \pmod{\text{ord}(a)}$.

EXAMPLE 21.4

(a) Compute all the solutions to the exponential equation $3^x \equiv 1 \pmod{17}$.

(b) Compute all the solutions to the exponential equation $9^x \equiv 1 \pmod{17}$.

PROPOSITION 21.3

If $a \in \mathbf{Z}$, $n \in \mathbf{Z}$, and $(a,n) = 1$, then all the numbers

$$a, a^2, a^3, \ldots, a^k = 1$$

are distinct modulo n.

Proof: Suppose that we have a repetition $a^j \equiv a^i \pmod{n}$, where $1 \leq i < j \leq k$. Thus, $a^{j-i} \equiv 1 \pmod{n}$. Since $1 \leq j - i \leq k$, we contradict the minimality of k.

To understand further what Proposition 3 is saying, it is worth looking at some examples.

EXAMPLE 21.5

For $n = 19$, and $a = 2$, we have $\text{ord}(2) = 18$.

2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	2^{13}	2^{14}	2^{15}	2^{16}	2^{17}	2^{18}
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Find the order of $2^2, 2^4, 2^5 \pmod{19}$.

THEOREM 21.1

$$\Big(a \in \mathbf{Z} \wedge n \in \mathbf{Z}_{\geq 1} \wedge (a,n) = 1\Big) \implies \left(\operatorname{ord}(a^m) = \frac{\operatorname{ord}(a)}{(\operatorname{ord}(a), m)}\right)$$

Proof: Let $\operatorname{ord}(a^m) = \ell$. We will show that $\ell = \frac{k}{(k,m)}$, where $k = \operatorname{ord}(a)$. Note that

$$a^{\ell m} \equiv (a^m)^\ell \equiv 1 \pmod{n}.$$

Thus, by Proposition 1 (Lecture 16), $k \mid \ell m$. Hence, there exists $q \in \mathbf{Z}$ such that $\ell m = kq$, but then

$$\ell \frac{m}{(k,m)} = \frac{k}{(k,m)} q.$$

Hence, $\frac{k}{(k,m)} \mid \ell \frac{m}{(k,m)}$, which implies that $\left(\frac{m}{(k,m)}, \frac{k}{(k,m)}\right) = 1$ by Proposition 2 (Lecture 3). It follows from Proposition 2 (Lecture 4) that

$$\frac{k}{(k,m)} \mid \ell.$$

On the other hand, we have

$$(a^m)^{\frac{k}{(k,m)}} \equiv (a^k)^{\frac{m}{(k,m)}} \equiv 1 \pmod{n}.$$

Thus, by Proposition 1 (Lecture 16), $\ell \mid \frac{k}{(k,m)}$. Thus, we conclude that $\ell = \frac{k}{(k,m)}$; that is,

$$\operatorname{ord}(a^m) = \frac{\operatorname{ord}(a)}{(\operatorname{ord}(a), m)}.$$

COROLLARY 21.2

$$\Big(a \in \mathbf{Z} \wedge n \in \mathbf{Z}_{\geq 2} \wedge k \in \mathbf{Z}_{\geq 1} \wedge (a,n) = 1\Big) \implies \Big(\operatorname{ord}(a^k) = \operatorname{ord}(a) \iff \big(k, \operatorname{ord}(a)\big) = 1\Big).$$

PROPOSITION 21.4

Define $\operatorname{ord}(a) = k$ *and* $\operatorname{ord}(b) = \ell$, *where* $a \in \mathbf{Z} \wedge n \in \mathbf{Z}_{\geq 2} \wedge (a,n) = 1 = (b,n) \wedge k, \ell \in \mathbf{Z}^+$.

$$(k,\ell) = 1 \implies \operatorname{ord}(ab) = k\ell.$$

EXERCISE 21.2

Prove Proposition 1.

Lambert was the first to look at primitive roots. In 1769, he conjectured that for any prime p, there was a number g such that $p \mid (g^{p-1} - 1)$, but $p \nmid (g^e - 1)$ for any $0 < e < p - 1$.

Euler was the first to use the term 'primitive root' in 1773 when he tried to prove Lambert's claim. However, his proof was not correct. Gauss, in 1801, gave two proofs of the existence of a primitive root for any prime p.

DEFINITION 21.2

An element $[a] \in \mathbf{Z}_n^*$ is called a primitive root if $\operatorname{ord}(a) = \varphi(n)$. In terms of congruences, let $a \in \mathbf{Z} \wedge n \in \mathbf{Z}_{\geq 2} \wedge (a,n) = 1$. If $\operatorname{ord}(a) = \varphi(n)$, then a is called a **primitive root** of modulo n.

Note that a primitive root modulo n is an element of $[a] \in \mathbf{Z}_n^*$ whose powers generate all $\mathbf{Z}_n^*$; that is, every element $[b] \in \mathbf{Z}_n^*$ can be written as $a^x \pmod{n}$ for some positive $x \in \mathbf{Z}$.

EXAMPLE 21.6

If $n = 5$, then $\varphi(5) = 4$. We see that 2 is the primitive root modulo 5 since

$$2^1 \equiv 2 \pmod 5$$
$$2^2 \equiv 4 \pmod 5$$
$$2^3 \equiv 3 \pmod 5$$
$$2^4 \equiv 1 \pmod 5.$$

Thus, $\operatorname{ord}(a) = 4$. For every integer relatively prime to 5, there is a power of 2 that is congruent.
We see that 4 is not a primitive root modulo 5 since

$$4^1 \equiv 4 \pmod 5$$
$$4^2 \equiv 1 \pmod 5.$$

Thus, $\operatorname{ord}(4) = 2$. Powers of $4 \pmod 5$ are only congruent to 1 or 4. There is no power of 4 that is congruent to 2 or 3.

THEOREM 21.2: Primitive Root Theorem

If p is prime, then there exists a root modulo p.

EXERCISE 21.3

Prove Theorem 2.

EXERCISE 21.4

Find a modulo n where no primitive roots exist.

Let us determine how many primitive roots exists.

PROPOSITION 21.5

If there is a primitive root modulo n, then the total number of primitive roots modulo n is $\varphi\big(\varphi(n)\big)$.

Proof: Let a be the primitive root modulo n, so that $\operatorname{ord}(a) = \varphi(n)$. Thus,

$$a, a^2, \ldots, a^{\varphi(n)} = 1$$

are all distinct. So every other integer relatively prime to n is a power of $a \pmod n$. The other primitive roots are those powers a^j in the list for which

$$\operatorname{ord}(a^j) = \varphi(n) = \operatorname{ord}(a).$$

According to Corollary 1, these powers a^j, where j from 1 to $\varphi(n)$ is coprime to $\varphi(n)$, and there are precisely $\varphi\big(\varphi(n)\big)$.

LECTURE 18 (PART I)
13th June

22 Costas Array

Here is a challenge. Given an $n \times n$ array, put dots into the centre of boxes such that

(1) Every row has exactly one dot.

(2) Every column has exactly one dot.

(3) If you draw all $\frac{n(n-1)}{2}$ lines segments, then any two lines that have the same slope, must have different length.

A grid satisfying all three conditions is called a **Costas array**.

The third condition is equivalent to: when a Costas array and a replica of itself are overlaid with an offset of an integer number of row and columns shifts such that 1 overlays another 1, then that will be the only 1s that overlay. In Costas array, we represent each entry either by the 1 for the dot or by 0 for the absence of dot.

EXAMPLE 22.1

A Costas array for $n = 5$ is:

1	0	0	0	0
0	0	0	1	0
0	1	0	0	0
0	0	1	0	0
0	0	0	0	1

EXERCISE 22.1

Draw a Costas array for $n = 3, 4, 6$.

John Costas and Edgar Gilbert independently introduced Costas arrays in 1965. To get a Costas array for $n = p - 1$, where p is prime, we will use the following algorithm. Gilbert at that time had discovered the Welch algorithm which was rediscovered by Lloyd Welch in 1982.

Welch Algorithm: Let a be a primitive root of p. Define the array $A_{i,j}$ by

$$A_{i,j} = \begin{cases} 1 & a^i \equiv j \pmod{p} \\ 0 & \text{otherwise.} \end{cases}$$

EXAMPLE 22.2

Draw a Costas array for $n = 4$.

Solution: We have $p = 5$ and a primitive root of 5 is $a = 3$. So, we have

$$\begin{aligned} 3^1 \equiv 3 \pmod{5} &\implies A_{1,3} = 1 \\ 3^2 \equiv 4 \pmod{5} &\implies A_{2,4} = 1 \\ 3^3 \equiv 2 \pmod{5} &\implies A_{3,2} = 1 \\ 3^4 \equiv 1 \pmod{5} &\implies A_{4,1} = 1. \end{aligned}$$

Therefore, the Costas array for $n = 4$ is:

0	0	1	0
0	0	0	1
0	1	0	0
1	0	0	0

EXERCISE 22.2

Draw a Costas array for $n = 10$.

23 Indices

The facts that every prime p has a primitive root combined with the fact that for any primitive root a of p, we have that

$$a, a^2, \ldots, a^{p-1} = 1$$

gives every number $1, 2, \ldots, p-1$ exactly once turns out to be rather useful.

Consider the powers of the primitive root 2 modulo 11:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	5	10	9	7	3	6	1

Now, rewrite this by ordering the second row as:

2^{10}	2^1	2^8	2^2	2^4	2^9	2^7	2^3	2^6	2^5
1	2	3	4	5	6	7	8	9	10

We can rewrite the first rows by just indicating the powers as:

10	1	8	2	4	9	7	3	6	5
1	2	3	4	5	6	7	8	9	10

If we now think about exponent laws, we get that addition of numbers in the first row, say $2+4=6$, corresponds to multiplication modulo 11 in the bottom row $4 \cdot 5 = 9$.

Gauss defined 'index' in 1801 to solve polynomial congruences. Jacobi published a table of indices for all primes powers less than 1000 in 1839.

DEFINITION 23.1

Let a be a primitive root of p, where p is prime. If $g \equiv a^\ell \pmod{p}$, then we say that ℓ is the index of g modulo p to the base a, and we write it as:

$$\ell = \mathcal{I}_a(g).$$

From the above example,

g	1	2	3	4	5	6	7	8	9	10
$\mathcal{I}_2(g)$	10	1	8	2	4	9	7	3	6	5

EXERCISE 23.1

Write an index table of g modulo $p=5$ to the base $a=3$, and an index table of g modulo p to the base $a=2$.

LEMMA 23.1

Let a be a primitive root of p, where p is prime.

$$a^b \equiv a^c \pmod{p} \iff b - c \equiv 0 \pmod{p-1}.$$

EXERCISE 23.2

Consider the following table of indices of g modulo 37 to the base 2:

g	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathcal{I}_2(g)$	36	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4	7	17
g	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$\mathcal{I}_2(g)$	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20	8	19	18

Compute $\mathcal{I}_2(8) + \mathcal{I}_2(9)$, $\mathcal{I}_2(8 \cdot 9)$, $2\,\mathcal{I}_2(3)$, and $\mathcal{I}_2(9)$.

NOTE: When calculating $\mathcal{I}_2(8) + \mathcal{I}_2(9)$, make sure that you are reducing modulo $p - 1$.

Thus, we can see that indices behave a lot like logarithms (we must be very careful about the modulus though!). We have the following properties.

PROPOSITION 23.1

If a is a primitive root of p, where p is prime, then we have

(1) $x \equiv y \pmod{p} \iff \mathcal{I}_a(x) \equiv \mathcal{I}_a(y) \pmod{p-1}$.

(2) $\mathcal{I}_a(a^r) \equiv r \pmod{p-1}$.

(3) $\mathcal{I}_a(a) = 1$.

(4) $\mathcal{I}_a(x \cdot y) \equiv \mathcal{I}_a(x) + \mathcal{I}_a(y) \pmod{p-1}$.

(5) $\mathcal{I}_a(x^k) \equiv k\,\mathcal{I}_a(x) \pmod{p-1}$.

EXAMPLE 23.1

Use the table of indices of g modulo 37 to the base 2 to solve the following:

(1) $x \equiv 3 \cdot 5 \pmod{37}$.

(2) $x \equiv 33 \cdot 29 \pmod{37}$.

(3) $x \equiv 17^{12} \pmod{37}$.

(4) $19x \equiv 23 \pmod{37}$.

Solution:

(1) $\mathcal{I}_2(3) = 26$ and $\mathcal{I}_2(5) = 23$, so we get

$$\mathcal{I}_2(3 \cdot 5) \equiv \mathcal{I}_2(3) + \mathcal{I}_2(5) \equiv 26 + 23 \equiv 13 \pmod{36}.$$

$\mathcal{I}_2(x) = 13 \implies x = 15$.

(2) $\mathcal{I}_2(17^{12}) \equiv 12\,\mathcal{I}_2(17) \equiv 12(7) \equiv 12 \pmod{36}$. Now, $\mathcal{I}_2(x) = 12 \implies x = 26$

(3) Note that

$$\begin{aligned} 19x &\equiv 23 \pmod{37} \\ \mathcal{I}_2(19x) &\equiv \mathcal{I}_2(23) \pmod{36} \\ \mathcal{I}_2(19) + \mathcal{I}_2(x) &\equiv 15 \pmod{36} \\ 35 + \mathcal{I}_2(x) &\equiv 15 \pmod{36} \\ \mathcal{I}_2(x) &\equiv -20 \pmod{36} \\ &\equiv 16 \pmod{36} \end{aligned}$$

$$\mathcal{I}_2(x) = 16 \implies x = 9.$$

Note: The Index is also known as discrete logarithm because the properties of indices and logarithm are same. Originally tables of indices, just like logarithm tables, were used to make numerical calculations much faster.

However, in recent years, indices have been revived for use in cryptography. In particular, if we are given a large prime p and two numbers a and g modulo p, then it is very difficult to find the exponent k such that

$$a^k \equiv g \pmod{p}.$$

This is called the discrete logarithm problem. One example of such a system is called the EIGamal cryptosystem.

WEEK 7
15th June

Midterm.

LECTURE 18 (PART II)
17th June

24 An Application to Communications Security

LECTURE 19
20th June

LECTURE 20
22nd June

25 Quadratic Congruences

Let $n \geq 3$ be a modulus and $a, b, c \in \mathbf{Z}$. We will now turn our attention to the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{n},$$

where $a, b, c \in \mathbf{Z}$, $n \nmid a$, and x is unknown modulo n.

In terms of equations in $\mathbf{Z}_n$,

$$[a]x^2 + [b]x + [c] = [0],$$

where $[a], [b], [c] \in \mathbf{Z}$, and x is an unknown residue class in $\mathbf{Z}_n$.

Note:

(1) For a quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{n}$, we require $n \nmid a$. Otherwise, the quadratic congruence collapse to the linear congruence $bx + c \equiv 0 \pmod{n}$.

(2) For $n = 2$, the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{n}$ collapses into a linear congruence. Indeed, by Fermat's Invariant (Corollary 1 Lecture 14), $x^2 \equiv x \pmod{2}$ regardless of x and so

$$ax^2 + bx + c \equiv (a + b)x + c \pmod{2}.$$

(3) For simplicity of interpretation, we will assume the n to be prime and denote it by p. If p is an odd prime (i.e., $p \neq 2$), then $\frac{p-1}{2} \in \mathbf{Z}$.

PROPOSITION 25.1

Let p be an odd prime, and $a, b, c, \in \mathbf{Z}$ with $p \nmid a$. The quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

has a solution if and only if the congruence

$$y^2 \equiv b^2 - 4ac \pmod{p}$$

has a solution. In that case $y \equiv 2ax + b \pmod{p}$.

Proof:

Proposition 1 tells us that solving the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

is equivalent to solving a simplifier quadratic congruence

$$y^2 \equiv d \pmod{p},$$

where $d = b^2 - 4ac$. The integer d is called the discriminant of the polynomial $ax^2 + bx + c$.

EXAMPLE 25.1

Solve $2x^2 + 18x + 3 \equiv 0 \pmod{23}$.

Solution: The discriminant of this quadratic polynomial modulo 23 is

$$18^2 - 4(2)(3) \equiv 300 \equiv 1 \pmod{23}.$$

According to Proposition 1, we should first solve

$$y^2 \equiv 1 \pmod{23}.$$

By inspection, we see that $y = 1$ and $y = 22$ are the solutions. According to Proposition 1, we need to solve

$$4x + 18 \equiv 1 \pmod{23}, \text{ and } 4x + 18 \equiv 22 \pmod{23}.$$

Solving them gives

$$x \equiv 1 \pmod{23}, \text{ and } x \equiv 13 \pmod{23},$$

which are the solutions of the given congruence.

In order to find solutions of $y^2 \equiv d \pmod{p}$, we need to understand which residue classes of $\mathbf{Z}_p$ are squares.

DEFINITION 25.1

Let p be an odd prime. A residue $[a]$ in $\mathbf{Z}_p$ is called a quadratic residue when

$$[a] \in \mathbf{Z}_p^* \text{ and } [a] = [b]^2 \text{ for some other residue } [b] \in \mathbf{Z}_p^*.$$

If no such $[b]$ exists, then $[a]$ is called a quadratic non-residue.
In terms of congruences, an integer a is a quadratic residue modulo p if

$$(p, a) = 1 \wedge \exists b \in \mathbf{Z}\ a \equiv b^2 \pmod{p} \wedge (b, p) = 1.$$

EXAMPLE 25.2

Find quadratic residues in $\mathbf{Z}_7^*$.

Solution: Note that

$$1^2 \equiv 1 \pmod 7$$
$$2^2 \equiv 4 \pmod 7$$
$$3^2 \equiv 2 \pmod 7$$
$$4^2 \equiv 2 \pmod 7$$
$$5^2 \equiv 4 \pmod 7$$
$$6^2 \equiv 1 \pmod 7$$

Thus, we can say that integers having quadratic residues modulo 11 are those that are congruent to $1, 2, 4$.

EXERCISE 25.1

Determine all quadratic non-residues modulo 17.

PROPOSITION 25.2

Let p be an odd prime. Then, there are exactly $\frac{p-1}{2}$ quadratic residues modulo p and exactly $\frac{p-1}{2}$ quadratic non-residues modulo p.

EXERCISE 25.2

Prove Proposition 1.

Detecting Quadratic Residues with Primitive Roots: Since p is an odd prime, by the Primitive Root Theorem (Theorem 2 Lecture 17), there exists a primitive root modulo p, say a, and by Proposition 2 (Lecture 17), the number of such primitive roots is $\varphi(p-1)$. Also, the powers

$$a, a^2, \ldots, a^{p-1}$$

are all distinct modulo p and exhausts $\mathbf{Z}_p^*$. By looking at k, we can decide whether a^k is a quadratic residue or not.

PROPOSITION 25.3

If a is a primitive root modulo p with $(a, p) = 1$ and $a^i \equiv a^j \pmod p$, then these exponents will be both even or both odd.

Proof:

LECTURE 21
24th June

For a simpler notation, let's write QR for a quadratic residue modulo p and NR for a quadratic non residue modulo p: From the Example 1 (Lecture 20), we see that we have

$$\text{QR} \cdot \text{QR} = \text{QR}$$
$$\text{QR} \cdot \text{NR} = \text{NR}$$
$$\text{NR} \cdot \text{NR} = \text{QR}.$$

Note that quadratic residues are the perfect squares of $\mathbf{Z}_p^*$ and you can easily get quadratic residues by squaring all the elements of $\mathbf{Z}_p^*$.

PROPOSITION 25.4

If p is an odd prime, then

(1) The product of two quadratic residues modulo p is a quadratic residue modulo p.

(2) The product of a quadratic residue modulo p and a quadratic non-residue modulo p is quadratic non-residue modulo p.

(3) The product of two quadratic non-residues modulo p is a quadratic residue.

Proof:

What does the multiplication rule of quadratic residues and quadratic non residues remind of you?

$$\begin{aligned} 1 \cdot 1 &= 1 \\ 1 \cdot (-1) &= -1 \\ (-1) \cdot (-1) &= 1. \end{aligned}$$

In 1798, the French Mathematician Adrien-Marie Legendre introduced a handy symbol to mark this distinction.

For an odd prime p, and $a \in \mathbf{Z}$ with $p \nmid a$, the **Legendre symbol**, $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & a \text{ is a QR modulo } p, \\ -1, & a \text{ is a NR modulo } p. \end{cases}$$

Note:

(1) Keep in mind that the Legendre symbol is not a fraction, even though it sort of look like one.

(2) 1 is a quadratic residue modulo p for any odd prime p; that is, $\left(\frac{1}{p}\right) = 1$.

(3) -1 might or might not be a quadratic residue, depending on the p. For example, $\left(\frac{-1}{19}\right) = -1$ and $\left(\frac{-1}{5}\right) = 1$.

(4) We can rewrite Proposition 1 using the Legendre symbol as

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

(5) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right)$ because the quadratic residue is the same for all congruent integers.

EXERCISE 25.3

Calculate $\left(\frac{3}{13}\right)$, $\left(\frac{11}{13}\right)$, and $\left(\frac{6}{17}\right)$.

The Proposition 1 suggest an Algorithm for calculating the Legendre polynomial $\left(\frac{a}{p}\right)$. First, we need to find the primitive root b modulo p and then determine the parity of x in $b^x \equiv a \pmod{p}$. Euler came up with a much simpler procedure.

PROPOSITION 25.5: Euler's Test

If p is an odd prime and $a \in \mathbf{Z}$ with $p \nmid a$, then

$$a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \pmod{p}.$$

Proof:

EXAMPLE 25.3

Does 79 have a quadratic residue modulo 31?

Solution: Note that $\frac{31-1}{2} = 15$ and by Euler's Test we reduce $79^{15} \pmod{31}$ (using the double-and-add algorithm). Note that $15 = 1 + 2 + 4 + 8$, and so $17^{15} = 17^1 \cdot 17^2 \cdot 17^4 + 17^8$. We have

$$17 \equiv 17,\ 17^2 \equiv 10,\ 17^4 \equiv 7,\ 17^8 \equiv 18 \pmod{31}.$$

Thus,

$$17^{15} = 17 \cdot 10 \cdot 7 \cdot 18 \equiv 30 \equiv -1 \pmod{31}.$$

According to Euler's test, 79 does not have a quadratic residue modulo 31. In the Language of the Legendre symbol we have found that

$$\left(\frac{79}{31}\right) = -1.$$

LECTURE 22
27th June

COROLLARY 25.1

If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4}, \\ -1, & p \equiv 3 \pmod{4}. \end{cases}$$

Proof:

PROPOSITION 25.6

There are infinitely many primes congruent to 1 modulo 4.

PROPOSITION 25.7

If p is an odd prime, then

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv 1, 7 \pmod{8}, \\ -1, & p \equiv 3, 5 \pmod{8}. \end{cases}$$

Proof:

EXERCISE 25.4

Using the technique in the proof of Proposition 2, show that 2 does not have a quadratic residue modulo 19.

Solution: Note that $19 \equiv 3 \pmod 8$, so $\left(\frac{2}{19}\right) = -1$ by Proposition 2.

26 The Law of Quadratic Reciprocity

We have solved the problem of finding $\left(\frac{a}{p}\right)$ for $a = -1$ and $a = 2$. Unfortunately, our method does for doing that does not exist for large values of a. We need a fast algorithm for calculating $\left(\frac{a}{p}\right)$ for any integer a and odd prime p with $p \nmid a$.

The Law of Quadratic Reciprocity was conjectured by Euler and Legendre in 1744. Gauss, in 1796, was the first to prove the Law of Quadratic Reciprocity, at the age of 19 and subsequently found at least five other proofs. He referred it as "The Golden Theorem." There are now over 240 published proofs (people are still publishing new proofs).

THEOREM 26.1: Law of Quadratic Reciprocity

If p and q are distinct odd prime numbers, then

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & p \equiv 1 \pmod 4 \vee q \equiv 1 \pmod 4, \\ -\left(\frac{q}{p}\right), & p \equiv 3 \pmod 4 \wedge q \equiv 3 \pmod 4. \end{cases}$$

The Law of Quadratic Reciprocity can be stated as:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

The proof is quite non-trivial and due to limitations of time we will not present it in class or in lecture notes as well. For the proof you can see Section 6.4 of "A taste of Number Theory" by Frank Zorzitto.

EXAMPLE 26.1

Calculate $\left(\frac{7}{109}\right)$.

Solution:

$$\begin{aligned} \left(\frac{7}{109}\right) &= \left(\frac{109}{7}\right) && 109 \equiv 1 \pmod 4 \\ &= \left(\frac{4}{7}\right) && 109 \equiv 4 \pmod 7 \\ &= \left(\frac{2}{7}\right)\left(\frac{2}{7}\right) && \text{Legendre symbol is multiplicative} \\ &= \left(\frac{2}{7}\right)^2 \\ &= 1. \end{aligned}$$

Thus, 7 is a quadratic residue modulo 109.

EXAMPLE 26.2

Calculate $\left(\frac{191}{839}\right)$.

Solution:

$$\begin{aligned}
\left(\frac{191}{839}\right) &= -\left(\frac{839}{191}\right) && 191 \equiv 3 \pmod 4 \wedge 839 \equiv 3 \pmod 4 \\
&= -\left(\frac{75}{191}\right) && 839 \equiv 75 \pmod{191} \\
&= -\left(\frac{5}{191}\right)^2\left(\frac{3}{191}\right) \\
&= -\left(\frac{5}{191}\right)^2\left(\frac{3}{191}\right) \\
&= -(1)\left(\frac{3}{191}\right) \\
&= \left(\frac{191}{3}\right) && 191 \equiv 3 \pmod 4 \wedge 3 \equiv 3 \pmod 4 \\
&= \left(\frac{2}{3}\right) && 191 \equiv 2 \pmod 4 \\
&= -1.
\end{aligned}$$

Thus, 191 is quadratic non-residue modulo 839.

EXERCISE 26.1

Calculate $\left(\frac{37603}{48611}\right)$ given that $37603 = 31 \cdot 1213$.

Solution:

$$\begin{aligned}
\left(\frac{37603}{48611}\right) &= \left(\frac{31}{48611}\right)\left(\frac{1213}{48611}\right) && \text{Legendre symbol is } \times \\
&= -\left(\frac{48611}{31}\right)\left(\frac{48611}{1213}\right) && 31 \equiv 3 \pmod 4 \wedge 48611 \equiv 3 \pmod 4,\ 1213 \equiv 1 \pmod 4 \\
&= -\left(\frac{3}{31}\right)\left(\frac{91}{1213}\right) && 48611 \equiv 3 \pmod{31},\ 48611 \equiv 91 \pmod{1213} \\
&= \left(\frac{31}{3}\right)\left(\frac{7}{1213}\right)\left(\frac{13}{1213}\right) && 3 \equiv 3 \pmod 4 \wedge 31 \equiv 3 \pmod 4 \\
&= \left(\frac{1}{3}\right)\left(\frac{1213}{7}\right)\left(\frac{1213}{13}\right) && 1213 \equiv 1 \pmod 4 \\
&= \left(\frac{2}{7}\right)\left(\frac{4}{13}\right) && 1213 \equiv 2 \pmod 7,\ 1213 \equiv 4 \pmod{13} \\
&= \left(\frac{2}{13}\right)^2 && 2^{\frac{7-1}{2}} \equiv 8 \equiv 1 \pmod 7 \text{ using Euler's Test} \\
&= (-1)^2 && 13 \equiv 5 \pmod 8 \text{ using Proposition 25.15} \\
&= 1.
\end{aligned}$$

EXAMPLE 26.3

Let p and q be distinct primes such that $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$. Prove that the equation $x^2 - qy^2 = p$ has no integer solution.

LECTURE 23
29th June

27 Sum of Squares

Recall that way back in Exercise 5 (Lecture 8) you were asked to make a conjecture to which primes in $\mathbf{Z}$ are also primes in $\mathbf{Z}[i]$. The conjecture is that a prime $p \in \mathbf{Z}$ is a prime in $\mathbf{Z}[i]$ if and only if p cannot be written as a sum of two squares. We are now finally in a position to figure out which primes can be written as a sum of two squares.

Look at a few numbers:

$$\begin{aligned} 1 &= 1^2 + 0^2 \\ 2 &= 1^2 + 1^2 \\ 4 &= 2^2 + 0^2 \\ 5 &= 2^2 + 1^2 \\ 8 &= 2^2 + 2^2. \end{aligned}$$

Note that 3, 6, and 7 are not expressible in this way.

PROPOSITION 27.1

If p is a Gaussian prime and $p \mid zw$ for some $z, w \in \mathbf{Z}[i]$, then $p \mid z$ or $p \mid w$.

THEOREM 27.1

If $n \equiv 3 \pmod 4$, then n is not a sum of two squares.

Proof:

Albert Girard was the first to make the observation, describing all positive integer numbers (not necessarily primes) expressible as the sum of two squares of positive integers; this was published in 1625. The statement that every prime p of the form $4n+1$ is the sum of two squares is sometimes called Girard's theorem. For his part, Fermat wrote an elaborate version of the statement (in which he also gave the number of possible expressions of the powers of p as a sum of two squares) in a letter to Marin Mersenne dated December 25, 1640: for this reason this version of the theorem is sometimes called Fermat's Christmas theorem:

THEOREM 27.2: Fermat's Christmas Theorem

If p is a prime such that $p \equiv 1 \pmod 4$, then there exists $a, b \in \mathbf{Z}$ such that

$$p = a^2 + b^2.$$

Proof:

Now, we know that when p is an odd prime, the $p = x^2 + y^2$ has a solution in the positive integers x and y if and only if $p \equiv 1 \pmod 4$. Notice this also has a solution when $p = 2$ since $2 = 1^2 + 1^2$. We would like to generalize this result to all $n \in \mathbf{Z}^+$.

PROPOSITION 27.2

If $m, n \in \mathbf{Z}$ are expressible as a sum of two squares, then so is mn.

Proof:

THEOREM 27.3

$n \in \mathbf{Z}^+$ is expressible as sum of two squares if and only if every prime factor which is congruent to $3 \pmod 4$ appears with an even power.

Due to time limitations we will not present the proof in class or in these lectures notes. If you would like to see the proof, see Section 7 in "A Taste of Number Theory" by Frank Zorzitto.

EXAMPLE 27.1

Can we express 490 as a sum of two squares? If yes, then find $x, y \in \mathbf{Z}$ such that $490 = x^2 + y^2$.

Solution: Note that $490 = 2 \cdot 5 \cdot 7^2$. Since $5 \equiv 1 \pmod 4$ and $7 \equiv 3 \pmod 4$ (appears with an even power), by Fermat's Christmas Theorem and Theorem 3, 490 is expressible as a sum of squares. Further,

$$\begin{aligned} 490 &= 7^2 \cdot 5 \cdot 2 \\ &= 7^2 \cdot (2^2 + 1^2) \cdot (1^2 + 1^2) \\ &= (7^2 + 0^2) \cdot (3^2 + 1^2) \\ &= 21^2 + 7^2. \end{aligned}$$

EXERCISE 27.1

Can we express $584820 = 2^2 \cdot 3^4 \cdot 5 \cdot 19^2$ as sum of two squares?

Solution: Since $2^2 = 4 = 2^2 + 0^2$, $3 \equiv 3 \pmod 4$ (appears with an even power; Fermat's Christmas Theorem), $5 \equiv 1 \pmod 4$ (Theorem 3), and $19 \equiv 3 \pmod 4$ (appears with an even power; Fermat's Christmas Theorem), then 584820 is expressible as a sum of squares. Hence,

$$\begin{aligned} 584820 &= 2^2 \cdot 3^4 \cdot 5 \cdot 19^2 \\ &= (2^2 + 0^2) \cdot (9^2 + 0^2) \cdot (2^2 + 1^2) \cdot (19^2 + 0^2) \\ &= 2^2 \cdot 9^2 \cdot 19^2 \cdot (2^2 + 1^2) \\ &= 2^2 \cdot 9^2 \cdot 19^2 \cdot 2^2 + 2^2 \cdot 9^2 \cdot 19^2 \cdot 1^2 \\ &= 4^2 \cdot 9^2 \cdot 19^2 + 2^2 \cdot 9^2 \cdot 19^2 \\ &= (\underbrace{4 \cdot 9 \cdot 19}_{684})^2 + (\underbrace{2 \cdot 9 \cdot 19}_{342})^2. \end{aligned}$$

$x^2 = 342 \wedge y^2 = 684 \iff 584820 = x^2 + y^2$ for $x, y \in \mathbf{Z}^+$.

WEEK 9 | FRIDAY

1st July

Holiday (Canada Day).

LECTURE 24

4th July

28 Multiplicative Functions

In this section, we will derive some formulas for $\phi(n)$ and show that $\phi(n)$ has an important property called multiplicatively. To put this in the proper context, discussion will be made on arithmetic functions, Dirichlet products, and the Mobius inversion formula.

DEFINITION 28.1

An arithmetic function is a function defined on the positive integers which takes in the real or complex numbers, that is, a function $f\colon \mathbf{Z}^+ \to \mathbf{C}$.

For example, $f\colon \mathbf{Z}^+ \to \mathbf{X}$ defined by $f(n) = \sin(n)$.
Some important arithmetic functions are:

(1) The constant function defined by $C(n) = 1$ for all $n \in \mathbf{Z}^+$.

(2) The indicator function defined by $I(n) = \begin{cases} 1, & n = 1, \\ 0, & \text{otherwise} \end{cases}$ for all $n \in \mathbf{Z}^+$.

(3) The identity function defined by $i(n) = n$ for all $n \in \mathbf{Z}^+$.

(4) The number of divisors function $\tau\colon \mathbf{Z}^+ \to \mathbf{Z}^+$ defined by

$$\tau(n) = \text{the number of positive divisors of } n = \sum_{d|n} 1.$$

(5) The sum of divisors function $\sigma\colon \mathbf{Z}^+ \to \mathbf{Z}^+$ defined by

$$\sigma(n) = \text{sum of the positive divisors of } n = \sum_{d|n} d.$$

(6) For a fixed odd prime p, the Legendre symbol is arithmetic function denoted by λ_p.

$$\lambda_p(n) = \left(\frac{n}{p}\right).$$

(7) The Euler phi function φ is an arithmetic function defined as

$$\varphi(n) = \text{the number of units of } \mathbf{Z}_n.$$

Also, $\varphi(n) =$ the number of integers from 1 to n that are coprime to with n.

DEFINITION 28.2

An arithmetic function f is known as a **multiplicative function** if

$$f(mn) = f(m)f(n)\ \forall m, n \in \mathbf{Z}^+ \wedge (m, n) = 1.$$

The constant function C, indicator function I, and the identity function i are multiplicative.

PROPOSITION 28.1

Let f and g be the multiplicative functions. Then,

i. $f(1) = 1$.

ii. The function f is fully determined by its values at prime powers.

iii. fg is also multiplicative.

Proof: Directly follows from Definition 2.

DEFINITION 28.3

If f is an arithmetic function, then the divisor sum of f is defined as

$$[D(f)](n) = \sum_{d|n} f(d),$$

where $\sum_{d|n}$ means to sum over all the positive divisors of a positive integer n. The divisor sum of f is evaluated at a positive integer n takes the positive divisors of n, plugs them into f, and adds the results. A similar convention will hold for products.

Remark: Notice the divisor sum is a function which takes an arithmetic function as input and produces an arithmetic function as output.

EXAMPLE 28.1

Suppose $f : \mathbf{Z}^+ \to \mathbf{Z}^+$ defined by $f(n) = n^2$. Compute $[D(f)](12)$.

Solution: $[D(f)](n)$ is the sum of divisor of n, so

$$[D(f)](12) = \sum_{d|12} n^2 = 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2 = 210.$$

PROPOSITION 28.2

If m and n are coprime positive integers, then every positive divisor d of their product mn comes from a unique pair a and b such that

$$a \mid m \wedge b \mid n \wedge ab = d.$$

Proof:

THEOREM 28.1

If f is a multiplicative function $D(f)$ defined by

$$[D(f)](n) = \sum_{d|n} f(d)$$

is also multiplicative.

Proof:

PROPOSITION 28.3

The functions τ and σ are multiplicative functions.

Proof:

THEOREM 28.2

The Euler function φ is multiplicative, that is,

$$\varphi(mn) = \varphi(m)\varphi(N)\ \forall m, n \in \mathbf{Z}^+ \wedge (m, n) = 1.$$

Proof:

Formula for $\tau(n)$

We can get a formula for $\tau(n)$ assuming τ is multiplicative and considering the unique factorization of n into primes. If $n = p^e$, then $\tau(n) = e + 1$. Therefore, if $n = p_1^{e_1} \cdots p_k^{e_k}$, then

$$\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

since τ is multiplicative.

Formula for $\sigma(n)$

We can get a formula for $\sigma(n)$ assuming σ is multiplicative and considering the unique factorization of n into primes. If $n = p^e$, then

$$\sigma(n) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}.$$

If $n = p_1^{e_1} \cdots p_k^{e_k}$, then

$$\sigma(n) = \left(\frac{p_1^{e_1+1} - 1}{p_1 - 1}\right) \cdots \left(\frac{p_k^{e_k+1} - 1}{p_k - 1}\right)$$

since σ is multiplicative.

Formula for $\varphi(n)$

We can get a formula for $\tau(n)$ assuming φ is multiplicative and considering the unique factorization of n into primes. If $n = p^e$, then the only numbers not coprime to p^e are the multiples of p, and there are $\frac{p^e}{p} = p^{e-1}$ of these. Thus,

$$\varphi(p^e) = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right).$$

If $n = p_1^{e_1} \cdots p_k^{e_k}$, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_k}\right).$$

EXAMPLE 28.2

Find $\varphi(20)$.

Solution: Since $20 = 2^2 \cdot 5$, we have

$$\varphi(20) = 20\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 8.$$

Theorem 1 (Lecture 24) applied to Euler's function gives us a nice non-obvious fact.

PROPOSITION 28.4

For every positive integer n,

$$\sum_{d|n} \varphi(d) = n.$$

Proof:

DEFINITION 28.4

If f and g are arithmetic functions, their Dirichlet product is

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

PROPOSITION 28.5

Let f, g, and h be arithmetic functions. Then,

(a) $f * g = g * f$.

(b) $(f * g) * h = f * (g * h)$.

(c) $f * I = I * f = f$.

(d) $f * C = D(f) = C * f$.

Proof:

PROPOSITION 28.6

The Dirichlet product of two multiplicative functions is again multiplicative.

DEFINITION 28.5

The Mobius function μ is the arithmetic function defined by

$$\mu(n) = \begin{cases} 1, & n = 1, \\ (-1)^k, & n = p_1 p_2 \cdots p_k \quad \text{(i.e., } n \text{ is a product of distinct primes)}, \\ 0, & \text{otherwise (i.e., a prime repeats itself in the factorization of } n). \end{cases}$$

For example,

- $28 = 2^2 \cdot 7$, so $\mu(28) = 0$.
- $46 = 2 \cdot 23$, so $\mu(46) = (-1)^2 = 1$.
- $30 = 2 \cdot 3 \cdot 5$, so $\mu(30) = (-1)^3 = -1$.

EXERCISE 28.1

Construct a table of values of $\mu(n)$ for $n = 1, 2, \ldots, 12$. Further, calculate $\sum_{d|n} \mu(d)$ for $n = 1, 2, \ldots, 12$.

EXERCISE 28.2

Prove that the Mobius function is multiplicative.