3 Congruence arithmetic

3.1 Congruence mod n

As we said before, one of the most basic tasks in number theory is to factor a number a. How do we do this? We start with smaller numbers and see if they divide a.

You have probably know some basic divisibility tests:
2, 5, 10 — check last digit
3, 9 — check sum of digits
4, 25 — check last two digits
11 — check sum of odd vs even digits

The natural way to explain these tests (and find new ones) is by a more refined approach to divisibility: congruences. Instead of just saying a number a is divisible or not by some number m, it is helpful to look at the remainder, denoted $a \bmod n$.

Example.

$$0 \bmod 4 = 0$$
$$1 \bmod 4 = 1$$
$$2 \bmod 4 = 2$$
$$3 \bmod 4 = 3$$
$$4 \bmod 4 = 0$$
$$5 \bmod 4 = 1$$
$$6 \bmod 4 = 2$$
$$7 \bmod 4 = 3$$
$$8 \bmod 4 = 0$$

Definition 3.1. *We say a is* **congruent** *to b modulo n, and write $a \equiv b \bmod n$ if the remainders $a \bmod m$ and $b \bmod n$ are equal, i.e., if $n|b-a$.*

Example. $1003 \equiv 999 \bmod 4$.

3.2 Congruence classes and their arithmetic

Definition 3.2. *The* **congruence class** *of $a \pmod n$ is*

$$n\mathbb{Z} + a = \{nk + a : k \in \mathbb{Z}\}.$$

Note: this is the set of all numbers which are congruent to $a \bmod n$.

Proof: If $b \in n\mathbb{Z} + a$ then $b - a = nk$ for some k so $n|b-a$, i.e., $b \equiv a \bmod n$. Conversely $b \equiv a \bmod n$ precisely means $b - a = nk$ for some k, i.e., $b \in n\mathbb{Z} + a$.

Example. $2\mathbb{Z} = \{$*even numbers*$\}$ *and* $2\mathbb{Z} + 1 = \{$*odd numbers*$\}$. *Note: the $n\mathbb{Z} + a$ representations for congruence classes are not unique: e.g.,* $2\mathbb{Z} = 2\mathbb{Z} + 6$ *and* $2\mathbb{Z} + 1 = 2\mathbb{Z} - 1$.

Example. $n\mathbb{Z} = \{$*all numbers divisible by n*$\}$.

Example. $4\mathbb{Z}+1 = \{\ldots -7, -3, 1, 5, 9, \ldots\}$

Thus we see congruences mod n partition the integers into n "evenly distributed" classes, generalizing the notion of even and odd.

Observe that if $x \bmod n = a$ and $y \bmod n = b$, then $x + y \bmod n = (a + b) \bmod n$. I.e., if $x \in n\mathbb{Z} + a$ and $y \in n\mathbb{Z} + b$ then $x + y \in n\mathbb{Z} + (a + b)$. Hence *congruence classes respect addition.* They also respect multiplication: if $x = nk + a$ and $y = nl + b$ then

$$xy = n^2kl + nla + nkb + ab \in n\mathbb{Z} + ab.$$

Hence we can work with the operations of $+$ and $\times$ mod n just as with the integers.

Example. *Addition on a 12 hour clock. 5 hours after 8:00 is 1:00. Using congruences, we can write this as* $8 + 5 \equiv 1 \bmod 12$.

Example. *Let* $n = 2, 5$ *or* 10. *Write* $a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$. *Then*

$$a \equiv (a_k \cdot 0 + a_{k-1} \cdot 0 + \cdots + a_1 \cdot 0 + a_0) \equiv a_0 \bmod n$$

since $10 \equiv 1 \bmod n$. *This explains why it suffices to check the last digit for divisibility by* $n = 2, 5, 10$.

Example. *Let* $n = 3$ *or* 9. *Write* $a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$. *Then*

$$a \equiv (a_k + a_{k-1} + \cdots + a_1 + a_0) \equiv \bmod n$$

since $10 \equiv 1 \bmod n$. *Hence a number is divisible by* $n = 3$ *if and only if the sum of its digits are, and the same is true for* $n = 9$.

Exercise 3.1. *Exercises 3.1.3, 3.1.4 (no proof needed for 3.1.4).*

Exercise 3.2. *Write* $a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$. *Prove that* a *is divisible by 11 if and only if the sum of the odd digits (*a_k *where* k *odd) minus the sum of the even digits (*a_k *where* k *even) is. (Hint: see Exercises 3.2.2, 3.2.3.)*

There are several methods for testing divisibility by 7, though they are more complicated. Can you figure any out?

A more algebraic approach.

Denote the set of congruence classes mod n by $\mathbb{Z}/n\mathbb{Z}$.

Definition 3.3. *We can define addition and multiplication in* $\mathbb{Z}/n\mathbb{Z}$ *as follows. The sum of two congruence classes is given by*

$$(n\mathbb{Z} + a) + (n\mathbb{Z} + b) = n\mathbb{Z} + (a + b).$$

The product is given by

$$(n\mathbb{Z} + a)(n\mathbb{Z} + b) = n\mathbb{Z} + ab.$$

Note: The idea of congruence arithmetic is very simple. The integers modulo n (i.e., the remainders) are $0, 1, \ldots, n-1$. For example for $n = 7$ we would like to say that

$$5 \bmod 7 + 3 \bmod 7 = 1.$$

However this is technically incorrect as

$$5 \bmod 7 + 3 \bmod 7 = 5 + 3 = 8 \neq 1.$$

In other words, usual integer addition doesn't make sense on the integers mod n. So one approach is to write equations as $\bmod n$ equivalence relations, e.g.,

$$5 + 3 \equiv 8 \equiv 1 \bmod 7.$$

However, by defining addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ (equivalence classes), we can use the tools of modern algebra to study congruence arithmetic. In particular, we have made $\mathbb{Z}/n\mathbb{Z}$ into a what is called a *ring* (formal definition later). In this way we would write our above equation as

$$(7\mathbb{Z} + 5) + (7\mathbb{Z} + 3) = 7\mathbb{Z} + 8 = 7\mathbb{Z} + 1.$$

In practice however, it is cumbersome to write elements of $\mathbb{Z}/n\mathbb{Z}$ as $n\mathbb{Z} + a$. So we will often refer to elements of $n\mathbb{Z}$ (e.g., class $n\mathbb{Z} + a$) by a representative of the class (e.g., a). For instance, we may refer to the class $7\mathbb{Z} + 6$ as the element 5 in $\mathbb{Z}/7\mathbb{Z}$, or we might call it the element -2 in $\mathbb{Z}/7\mathbb{Z}$ depending on which is convenient, with it being understood that we mean the class of integers containing that number. Nevertheless, to avoid confusion we will not write *explicit* equations in the form, say $5^2 = 4$ (in $\mathbb{Z}/7\mathbb{Z}$), but rather in congruence notation: $5^2 \equiv 4 \pmod 7$.

Example. *Write down addition and multiplication tables for* $\mathbb{Z}/5\mathbb{Z}$.

Exercise 3.3. *Write down addition and multiplication tables for* $\mathbb{Z}/6\mathbb{Z}$.

3.3 Inverses mod p

Assume $n > 1$.

Definition 3.4. *We say a is* **invertible** *mod n if there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod n$. In this case b is called the* **(multiplicative) inverse** *of a* $(\bmod n)$.

Note that this only depends on the congruence class, i.e., if $a \equiv b \bmod n$, then a is invertible mod n if and only if b is.

In $\mathbb{Z}$ only $a = \pm 1$ are invertible (in the same sense: $\exists a^{-1} \in \mathbb{Z}$), however we saw in $\mathbb{Z}/5\mathbb{Z}$, every non-zero element is invertible. This means the non-zero classes mod 5 form an *abelian group.*

Definition 3.5. *Let G be a set with a* binary operation $\cdot$ *. , i.e., $\cdot$ is a function from $G \times G \to G$, expressed as $(g, h) \mapsto g \cdot h$. If G satisfies the following properties,*

(i) $\cdot$ is associative: $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ for all $g, h, k \in G$;

(ii) there is an identity *$1 \in G$ such that $1 \cdot g = g \cdot 1 = g$ for all $g \in G$;*

(iii) every $g \in G$ has an inverse *g^{-1} such that $g^{-1} \cdot g = g \cdot g^{-1} = 1$;*

then we say $(G, \cdot)$ (or just G) is a **group**. *If (i) through (iii) and*

(iv) $\cdot$ is commutative: $g \cdot h = h \cdot g$ for all $g, h \in G$

also hold, we say $(G, \cdot)$ (or just G) is an **abelian group**. *When the operation is understood, we typically write gh for $g \cdot h$.*

Note: We will not prove the following elementary facts, but $1 \cdot g = g$ for all g is equivalent to $g \cdot 1 = g$ for all g, and $g^{-1}g = 1$ is equivalent to $gg^{-1} = 1$, so one does not need to check multiplications both ways. (This is of course trivial when G is abelian—our primary case of interest.) Also conditions (ii) and (iii) defining the identity and the inverse of an element imply that such elements will be unique.

The *finite abelian groups* are the simplest class of groups and have a simple characterization. If G is a finite group with n elements, we say it is a finite group of **order** n, and write $|G| = n$. In case you are not familiar with groups, here are some examples.

Example. *$(\mathbb{Z}, +)$ is an abelian group. So is $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$, but $(\mathbb{N}, +)$ is not (see below).*

Example. *$(\mathbb{Z}/n\mathbb{Z}, +)$ is an finite abelian group of order n.*

Exercise 3.4. *Rewrite what properties (i) through (iv) mean when our operation is written as $+$ (called additive) and not $\cdot$ (called multiplicative). Which properties fail for $(\mathbb{N}, +)$? What is the (additive) inverse of $8\mathbb{Z} + 5$ in the group $(\mathbb{Z}/8\mathbb{Z}, +)$?*

Example. *(n-th roots of unity) Fix n. Let $U_n = \left\{e^{2\pi ik/n} : 0 \leq k < n\right\}$. Then, with the standard multiplication, U_n is a finite abelian group of order n. It has the same structure (is "isomorphic" to) $(\mathbb{Z}/n\mathbb{Z}, +)$, the only difference being one group is written with multiplicative notation and one with additive notation.*

Example. *(dihedral groups) Fix $n > 2$. Let P be a regular polygon with n vertices. The the set of automorphisms of P, namely the rotations and reflections which map P to itself, form a finite* non-abelian *group of order $2n$ called D_{2n}, where the operation is composition.*

Example. *(symmetric groups) Let S_n be the set of permutations of $\{1, 2, \ldots, n\}$. Then S_n is a finite group of order $n!$ with the composition operation. It is non-abelian for $n > 2$.*

Example. *$\mathbb{Q}^\times = \mathbb{Q} - \{0\}$ is an infinite abelian group with multiplication. So is $\mathbb{R}^\times$ and $\mathbb{C}^\times$. Similarly, the positive rational (or reals) also are.*

Example. *Let $\mathrm{SL}(2, \mathbb{Z}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1\right\}$. This is an infinite non-abelian group with usual matrix multiplication, and is an important group in number theory.*

Okay, so those were some examples. Basically, a group (in multiplicative notation) is a collection of objects that you can multiply and divide, and has "1." If the multiplication is commutative (which it is for numbers, but not in general for groups of functions or matrices), we say it is abelian (after Niels Abel).

We are interested in the invertible elements mod n, or equivalently, the invertible elemtns of $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{n\mathbb{Z} + a \in \mathbb{Z}/n\mathbb{Z} : a \text{ invertible mod } n\}.$$

Exercise 3.5. *Prove $(\mathbb{Z}/n\mathbb{Z})^\times$ is a finite abelian group. You may take for granted that multiplication is well defined on $\mathbb{Z}/n\mathbb{Z}$ (from the previous section) and associative, though you should say a sentence about why it is well defined on $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Before tackling $(\mathbb{Z}/n\mathbb{Z})^\times$ in general (as in, what are they? how many are there?) we first deal with the case n is prime.

Proposition 3.6. *Let p be prime. Then $(\mathbb{Z}/p\mathbb{Z})^\times$ is the set of non-zero classes in $\mathbb{Z}/p\mathbb{Z}$, i.e., it is a finite abelian group of order $p-1$.*

(By the zero class, we mean $p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$.)

Proof. First note that the zero class $\mathbb{Z}/p\mathbb{Z}$ cannot be invertible. For if it were, that would mean 0 is invertible mod p, but there is no b such that $0 \cdot b \equiv 1 \bmod p$.

Now we want to show any other class $p\mathbb{Z} + a$ is invertible, i.e., for any $a \not\equiv 0 \bmod p$, show a is invertible mod p. Since $p \nmid a$ and p is prime, $\gcd(a, p) = 1$. Thus Section 2.3 implies there exist $m, n \in \mathbb{Z}$ such that

$$ma + np = \gcd(a, p) = 1.$$

Hence $ma \equiv 1 \bmod p$ and m is the inverse of p. □

This statement says that any non-zero class in $\mathbb{Z}/p\mathbb{Z}$ is invertible, which implies $\mathbb{Z}/p\mathbb{Z}$ is a *field* with $+$ and $\cdot$, for those of you that have seen fields before.

Note that the proof shows we can determine the inverse of a mod p by the extended Euclidean algorithm.

A little group theory.

Definition 3.7. *Let $(G, \cdot)$ be a group. Let H be a subset of G. If $(H, \cdot)$ is also a group then H is called a* **subgroup** *of G. The* **(left) cosets** *of H in G are the subsets of G of the form*

$$gH = \{gh : h \in H\}, \quad g \in G.$$

Example. $n\mathbb{Z} \subseteq \mathbb{Z}$.

Just as congruences mod n partition $\mathbb{Z}$ into n different classes, we will see that the cosets partition G into a certain number of different classes (which we now call cosets). Let us first look at a few more examples.

Example. $U_2 \subseteq U_4$.

Example. $U_2, U_3 \subseteq U_6$.

Example. $H = \{1\} \subseteq G$.

Example. $H = G \subseteq G$.

Proposition 3.8. (Lagrange's theorem) *If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.*

Proof. First note that any the size of any coset gH is $|H|$: if $h, h' \in H$, then

$$gh = gh' \implies g^{-1}gh = g^{-1}gh' \implies h = h',$$

hence for a fixed g, all the products gh are distinct.

Now we claim that any two distinct g_1H and g_2H are disjoint. For if they intersect, then for some $h_1, h_2 \in H$, we have $g_1h_1 = g_2h_2$. We can write any $h \in H$ as $h_1h_1^{-1}h$, so

$$g_1h_1 = g_2h_2 \implies g_1h = g_1h_1h_1^{-1}h = g_2(h_2h_1^{-1}h) \in g_2H,$$

i.e., any element of g_1H must be inside g_2H also. But since the have the same size ($|H|$), we must have $g_1H = g_2H$, proving the claim.

Hence the cosets $\{gH\}$ partition G into disjoint subsets, all of size $|H|$. In particular there must be $|G|/|H|$ cosets, which proves Lagrange's theorem. □

Exercise 3.6. *Let $G = (\mathbb{Z}/7\mathbb{Z})^\times$. We represent the elements of G by $1, 2, \ldots, 6$.*

(i) Write down the multiplication table for G.

(ii) Let $H = \{1, 6\}$. Show H is a subgroup of G. (It suffices to check H is closed under multiplication and each element of H has an inverse in H. In other words, you may use the first lemma of the next section.)

(iii) Determine the cosets of H in G.

(iv) Repeat (ii) and (iii) for the set $H = \{1, 2, 4\}$.

3.4 Fermat's little theorem

A basic way to test is something is a subgroup is

Lemma 3.9. *If G is a group and H is a nonempty subset of G, then H is a subgroup of G if and only if it is closed under multiplication and taking inverses.*

Proof. ($\Leftarrow$) Suppose H is closed under multiplication and taking inverses. Being closed under multiplication implies that the multiplication on G restricts to a well defined binary operation on H. Associativity holds because it does in G. If H is closed under inverses, then pick any $h \in H$ so $h^{-1} \in H$. (Here is where we need H nonempty.) By closure under multiplication $hh^{-1} = 1 \in H$. This takes care of all 3 properties required to be a group.

($\Rightarrow$) If H is a group, it is closed under multiplication and inverses by definition. □

Note this is similar to the result in linear algebra that something is a subspace of a vector space if and only if it is closed under addition and scalar multiplication.

Lemma 3.10. *Let G be a finite group and $a \in G$. Then (i) there is some $n \in \mathbb{N}$ such that $a^n = 1$. (ii) Take the smallest such n, called the* **order of** *a. Then $C = \left\{a, a^2, a^3, \cdots, \ , a^n\right\}$ is a subgroup of G of order n.*

Proof. (i) Since G is finite, and $a^k \in G$ for all $k \in \mathbb{N}$ there must be some $j, k \in \mathbb{N}$ with $j \neq k$ such that $a^j = a^k$. Assume $j < k$ and let $n = k - j$. Then $a^j a^n = a^j a^{k-j} = a^k = a^j$. Multiplying by $(a^j)^{-1}$, we see $a^n = 1$.

(ii) Let n be the order of a, i.e., $n \in \mathbb{N}$ is the smallest such that $a^n = 1$. Then the argument in (i) shows we can't have $a^j = a^k$ for $1 \leq j < k \leq n$—otherwise $a^{k-j} = 1$ but $k - j < n$. Hence C has precisely n elements.

By the previous lemma, to check it is a subgroup it suffices to check closure under multplication and inverses. Take any a^j and a^k in C (with $1 \leq j, k \leq n$). If $j + k \leq n$, $a^j a^k = a^{j+k} \in C$ trivially; if $j + k > n$, we see $a^j a^k = a^{j+k} = a^{j+k-n} a^n = a^{j+k-n} \in C$ since $1 \leq j + k - n \leq n$. Hence C is closed under multplication.

Note since $a^n = 1$, $(a^n)^{-1} = 1 = a^n \in C$. For any $1 \leq j < n$, we have $1 \leq n - j < n$. Then since $a^j a^{n-j} = a^n$ □

The group C in this lemma is called the **cyclic subgroup generated by** a because it consists only of elements that are powers of a single element a. (It is called cyclic because these powers cyclically repeat: $a^n = 1, a^{n+1} = a^n a = a, a^{n+2} = a^n a^2 = a^2, \ldots$.)

Exercise 3.7. *Check that the powers of a cyclically repeat in this example.*
(i) With the notation in the previous exercise (in $(\mathbb{Z}/7\mathbb{Z})^\times$), compute 3^k for $1 \leq k \leq 10$.
(ii) What is the cyclic subgroup of $(\mathbb{Z}/7\mathbb{Z})^\times$ generated by 3? What about generated by 2?

Proposition 3.11. (Fermat's little theorem) *If p is prime and $a \not\equiv 0 \bmod p$, then $a^{p-1} \equiv 1 \bmod p$.*

Proof. We have seen that $(\mathbb{Z}/p\mathbb{Z})^\times$ is an abelian group of order $p-1$. Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Fermat's little theorem is equivalent to the statement that $a^{p-1} = 1$.

Let C be the cyclic subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ generated by a. Now C has order n where $n \in \mathbb{N}$ is minimal such that $a^n = 1$. By Lagrange's theorem, $n = |C|$ divides $p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$. Hence we can write $p = 1 = mn$ for some m. Thus $a^{p-1} = a^{mn} = (a^n)^m = 1^m = 1$. □

Example. (Formula for inverses mod p**)** *Suppose* $\gcd(a, p) = 1$. *Then the inverse a^{-1} of a mod p is given by $a^{-1} \equiv a^{p-2} \bmod p$. Check: $a^{-1}a \equiv a^{p-2}a \equiv a^{p-1} \equiv 1 \bmod p$.*

Recall we saw in Section 1.5 that we can do exponentiation quickly. This means we can compute inverses mod p quickly this way. We also showed we can compute them quickly via the extended Euclidean algorithm in the last section. However that was an algorithm *and not a* formula. *In general, it will be more convenient to use this explicit formula.*

Exercise 3.8. *Use the formula $a^{-1} \equiv a^{p-2} \bmod p$ to compute the inverse of* 5 mod 11. *(Do this computation by hand.)*

3.5 Congruence theorems of Wilson and Lagrange

Proposition 3.12. (Wilson's theorem). *Let p be prime. Then $(p-1)! \equiv -1 \bmod p$.*

Proof. Note if $p = 2$ it is trivial since $1 \equiv -1 \bmod 2$. Suppose $p > 2$. By the previous section, we know every $1 \leq a \leq p-1$ is invertible mod p. If $x \equiv x^{-1} \bmod p$, then $x^2 \equiv 1 \bmod p$ so

$$x^2 - 1 \equiv (x-1)(x+1) \equiv 0 \bmod p,$$

i.e., $p|(x-1)$ or $p|(x+1)$. By the prime divisor property, this means

$$x \equiv \pm 1 \bmod p.$$

Hence the only (equivalence classes of) $1 \leq a \leq p-1$ which are their own inverses mod p are (the equivalence classes of) $a = 1$ and $a = p-1$.

Now we write

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \equiv -2 \cdot 3 \cdots (p-2) \bmod p.$$

However each of the remaining factors $2, 3, \ldots, p-2$ are invertible and none of them are their own inverses. Hence any factor above, e.g., 2, will cancel with its inverse, e.g., 2^{-1}, in the product above. □

Exercise 3.9. *Exercises 3.5.1, 3.5.2, 3.5.3. (Correction: 3.5.1 should say if $n > 5$ is not prime, show $n|(n-1)!$)*

Above, we proved the quadratic polynomial x^2-1 has at most two solutions (up to equivalence) mod p, given by 1 and $p-1$. These are distinct if and only if $p>2$, which is why we separated the case $p=2$ first. This is similar to the fact that a polynomial of degree n has at most n solutions in $\mathbb{Z}$ (or $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$). This is also true for $\mathbb{Z}/p\mathbb{Z}$.

Proposition 3.13. (Lagrange) *Let $P(x)$ be a polynomial of degree n over $\mathbb{Z}$ and p be prime. Then $P(x)\equiv 0$ has at most n solutions mod p (i.e., in $\mathbb{Z}/p\mathbb{Z}$).*

Proof. If $P(x)\equiv 0 \bmod p$ has no solutions we are done. Otherwise, let $x=r$ be a solution and write

$$P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0.$$

Then

$$P(x)-P(r)\equiv a_n(x^n-r^n)+a_{n-1}(x^{n-1}-r^{n-1})+\cdots a_1(x-r)\equiv (x-r)Q(x) \bmod p$$

for some polynomial $Q(x)$ of degree $n-1$. This is because we can factor out an $(x-r)$ from any x^j-r^j to get a polynomial of degree $j-1$ over $\mathbb{Z}$.

However, since $x=r$ is a solution to $P(x)\equiv 0 \bmod p$,

$$P(x)\equiv P(x)-P(r)\equiv (x-r)Q(x) \bmod p.$$

So if x is any solution to $P(x)\equiv 0 \bmod p$, we have either $p|(x-r)$ or $p|Q(x)$ by the prime divisor property. Thus any solution not equivalent to r mod p, must be a solution of the degree $n-1$ equation

$$Q(x)\equiv 0 \bmod p.$$

Hence the number of solutions to $P(x)\equiv 0 \bmod p$ is one plus the number of solutions to $Q(x)\equiv 0 \bmod p$. Applying our argument for $P(x)$ to $Q(x)$, we can inductively reduce the problem down (i.e, use descent) to the case $n=1$, where the result is trivial. □

It often happens that $P(x)=0$ will have *more* solutions mod p than in $\mathbb{Z}$

Exercise 3.10. *Let $P(x)=x^2+1$. Clearly $P(x)=0$ is not solvable in $\mathbb{Z}$. However $P(x)\equiv 0 \bmod 5$ is solvable mod 5. Determine all solutions.*

3.6 Inverses mod k

When k is not prime, not every non-zero class mod k is invertible. For example 2 is not invertible mod 4: it is immediate from the definition that $2k\equiv 0,2 \bmod 4$.

Proposition 3.14. *a is invertible mod k if and only if $\gcd(a,k)=1$.*

Proof. ($\Rightarrow$) a invertible mod k means $ma\equiv 1 \bmod k$ for some m, i.e., $ma\in k\mathbb{Z}+1$, i.e., for some n, $ma+nk=1$. Since any common divisor of a and k must then divide 1, $\gcd(a,k)=1$.

($\Leftarrow$). $\gcd(a,k)=1$ implies $ma+nk=1$ for some $m,n\in\mathbb{Z}$. Reducing this mod k gives $ma\equiv 1 \bmod k$. □

Example. *$(\mathbb{Z}/8\mathbb{Z})^\times$ consists of (the classes of) $1,3,5,7$. Note that every element is it's own inverse, i.e., every element satisfies $x^2=1$ (in contrast to the mod p case). Hence $(\mathbb{Z}/8\mathbb{Z})^\times$ is non-cyclic (not generated by the powers of a single element) abelian group of order 4.*

Exercise 3.11. *For $2 \leq k \leq 7$ and $k = 9$, do the following. Write down the elements in $(\mathbb{Z}/k\mathbb{Z})^\times$ and state the order of the group. For each $a \in (\mathbb{Z}/k\mathbb{Z})^\times$, find the smallest n such that $a^n = 1$. Determine if $(\mathbb{Z}/k\mathbb{Z})^\times$ is cyclic or not. If it is cyclic, state an element that generates the group.*

Definition 3.15. *The* **Euler phi function** *is*

$$\phi(k) := \#\left\{1 \leq a \leq k-1 : \gcd(a,k) = 1\right\}.$$

Hence the proposition tells us

$$|(\mathbb{Z}/k\mathbb{Z})^\times| = \phi(k).$$

Many introductory number theory courses will spend a fair amount of time studying $\phi(k)$ and the structure of $(\mathbb{Z}/k\mathbb{Z})$. We will limit our study of $\phi(k)$ to the following. We already showed for p prime $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$, so $\phi(p) = p-1$.

Exercise 3.12. *Show $\phi(p^j) = p^{j-1}(p-1)$ for $j \geq 1$. (Exercises 3.6.1, 3.6.2, 3.6.3.)*

Exercise 3.13. *We will show in Chapter 9 that if m and n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$. Check this in the special cases (i) $m = 3$ and $n = 5$ (Exercise 3.6.4), and (ii) $m = 2$ and n is an odd prime.*

These two results show that we can determine $\phi(k)$ from its prime factorization.

Example. $\phi(3^3 \cdot 5) = 3^2(3-1)(5-1) = 9 \cdot 8 = 72$.

Exercise 3.14. *Determine $\phi(60)$.*

Proposition 3.16. (Euler's theorem) *For any invertible $a \bmod k$, we have $a^{\phi(k)} \equiv 1 \bmod k$*

Exercise 3.15. *Following the proof of Fermat's little theorem, prove Euler's theorem in the same way.*

3.7 Quadratic Diophantine equations

We can now use congruence arithmetic to say some things about *non-existence* of solutions of Diophanine equations.

Example. *$x^2 + y^2 = p$ has no solution for p of the form $4n + 3$.*

Example. *$x^2 + 2y^2 = p$ has no solution for p of the form $8n + 5$ or $8n + 7$.*

Example. *$x^2 + 3y^2 = p$ has no solution for p of the form $3n + 2$.*

Though p was not necessarily prime in the examples above, we can reduce the question of which numbers are of the form $x^2 + y^2$, etc., to the question of which primes are. This is because

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2,$$

i.e., if two numbers are sums of two squares, so is their product.

On the other hand is much harder is to show, for example, that any prime of the form $4n + 1$ is a sum of two squares, and one *cannot* do this with simple congruences.

Exercise 3.16. *Exercise 3.7.1.*

Exercise 3.17. *Show that if $p = x^2 + 4y^2$, then p is of the form $4n$ or $4n + 1$.*

Exercise 3.18. *Using congruences, prove that $k^3 + 2k$ is always divisible by 3.*

Exercise 3.19. *Show that if $p = x^3 + y^3$, then p is not of the form $9n + 4$ or $9n + 5$.*

3.8 *Primitive roots

Note that

$$1/3 = 0.3333\cdots$$
$$1/7 = 0.142857\ 142857\cdots$$
$$1/13 = 0.076923\ 076293\cdots$$

These are all periodic, with period lengths 1, 6, 6.

Proposition 3.17. *The decimal expansion of $x \in \mathbb{R}$ is periodic if and only if $x \in \mathbb{Q}$.*

The proof is not difficult but we will omit it. Note the expansion $1/2 = 0.5$ is considered periodic with period length 1 because after the 5, it repeats with zeroes: $1/2 = 0.50000000\ldots$.

Definition 3.18. *Suppose we have the decimal expansion $1/n = 0.\overline{a_1a_2a_3\cdots a_r}$. Then $1/n$ is called* **strictly periodic**. *The smallest such r is called the* **period length**.

Note $1/n$ is not always strictly periodic: $1/2 = 0.5\overline{0}$ and $1/6 = 0.1\overline{6}$. From now on, *assume $1/n$ is strictly periodic.*

Proposition 3.19. *If $1/n$ is strictly periodic with period length r, then 10 has order r in $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. Write $1/n = 0.\overline{a_1a_2a_3\cdots a_r}$. Then $10^r/n - 1/n = a_1a_2\cdots a_r \in \mathbb{Z}$ which implies that $10^r - 1 \in n\mathbb{Z}$, i.e., $10^r \equiv 1 \bmod n$. Note 10 cannot have order less than r, or else the period of $1/n$ would be smaller. □

Note that this implies the period $r \leq \phi(n)$. If $r = \phi(n)$ we say $1/n$ has **maximal period length**.

Definition 3.20. *We say a is a* **primitive root** mod n *if a generates $(\mathbb{Z}/n\mathbb{Z})^\times$, i.e., $(\mathbb{Z}/n\mathbb{Z})^\times = \{a^j\}$. Equivalently, a is a primitive root* mod n *if the order of a in $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\phi(n)$.*

Hence $1/n$ has maximal period length if and only if 10 is a primitive root mod n.

Conjecture 3.21. (Gauss) *There are infinitely many primes such that $1/p$ has maximal period length.*

Still unknown!

Exercise 3.20. *Without dividing, determine the period length of $1/11$. (For $p > 5$, we have $gcd(p, 10) = 1$, and one can show $1/p$ will be strictly periodic, so you may use the above proposition.) Check what the decimal expansion is on a calculator.*

3.9 *Existence of primitive roots

Let p be prime.

Lemma 3.22. *There are at most $\phi(n)$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order n.*

Proof. Suppose $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ has order n. Then $1, a, a^2, \ldots a^{n-1}$ are n distinct solutions to

$$x^n \equiv 1 \bmod p.$$

By the theorem of Lagrange in Section 3.5, there are at most n solutions to this equation, so $1, a, a^2, \ldots a^{n-1}$ are all of them.

On the other hand, if $\gcd(j, n) = d > 1$, then $j(n/d) = kn$ for some k. Hence

$$(a^j)^{(n/d)} \equiv a^{kn} \equiv (a^n)^k \equiv 1 \bmod p,$$

i.e., a^j has order $n/d < n$. In other words, a^j only has order n if $\gcd(j, n) = 1$. □

Lemma 3.23. $\sum_{d|N} \phi(d) = N$.

Proof. Write

$$\frac{1}{N}, \quad \frac{2}{N}, \quad \cdots, \quad \frac{N}{N}$$

in reduced form, e.g.,

$$\frac{1}{6}, \ \frac{2}{6}, \ \frac{3}{6}, \ \frac{4}{6}, \ \frac{5}{6}, \ \frac{6}{6} \longrightarrow \frac{1}{6}, \ \frac{1}{3}, \ \frac{1}{2}, \ \frac{2}{3}, \ \frac{5}{6}, \ 1.$$

Note that we will a reduced form $\frac{a}{d}$ with denominator d precisely $\phi(d)$ times. Thus counting this set in two ways give the result. □

Theorem 3.24. *There is a primitive root mod p.*

Proof. By Fermat's little theorem, $a^{p-1} \equiv 1 \bmod p$ for any $1 \leq a \leq p-1$. Hence each a has order d for some $d|p-1$. Thus the number of $1 \leq a \leq p-1$ with order less than $p-1$ is

$$\sum_{d|p-1 d<p-1} \phi(d) = p - 1 - \phi(p-1) < p - 1.$$

Hence some element has order $p-1 \bmod p$, i.e., is a primitive root. □

3.10 Discussion

Read it if you want to.

4 RSA

One important practical application to the material of the last chapter is the RSA cryptosystem.

Last night: Bob finds two big primes p and q walking down the street, and multiplies them together: $n = pq$ (blam!) He picks a random number e up at a bar, and posts e and n on his blog when he gets home.

***ν* playa:** Alice wants to send Bob a smokin' email m, without the fink sys admin Eve being able to read it. So she checks Bob's webpage, sees e and n, and sends him a cipha' $c \equiv m^e \bmod n$ (blam! blam!)

Back in the crib: Since Bob is tight with p and q, he knows $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$, and therefore $d \equiv e^{-1} \bmod \phi(n)$. So we he get's Alice's messsage, he's just like, whoa, I know what Alice is sayin':

$$c^d \equiv m^{ed} \equiv m^{k\phi(n)+1} \equiv m \bmod n \text{ (blam! blam! blam!)}$$

Computer lab: Eve is hatin' on Alice 'n Bob 'cuz she don't know her p's and q's, so she don't know $\phi(n)$ or m.