4. 2/13

4.1. *Rules for divisibility* We've been discussing divisors and long division. Have people heard the following rules for testing divisibility?

(1) 3 divides n if and only if it divides the sum of the digits of n.
(2) 4 divides n if and only if it divides the number formed by the last two digits of n.
(3) 5 divides n if and only if the last digit of n is 0 or 5.
(4) 9 divides n if and only if it divides the sum of the digits of n.

4.2. *Digits* What do we mean by a digit of n? It means the numbers $a_0, a_1, \ldots, a_k$ when we write n as

$$(*) \qquad n = 10^k a_k + \cdots + 10^2 a_2 + 10a_1 + a_0.$$

And similarly, after the decimal point, using negative powers of 10. This is called "expansion in base ten", or simply, decimal expansion.

Why do we write numbers this way, and not the way the Romans did? To write arbitrarily large numbers, the Romans would have needed to come up with arbitrarily many symbols.

4.3. Let us try to prove some of the divisibility rules.

Proof of the rule for 4. We want to show that, in the notation of (∗),

$$4 \text{ divides } n \iff 4 \text{ divides } 10a_1 + a_0.$$

The difference between n and $10a_1 + a_0$ is an expression X divisible by 10^2. Since $10^2 = 4(25)$, this expression is also divisible by 4. So if 4 divides n, then it divides $10a_1 + a_0 = n - X$, and if 4 divides $10a_1 + a_0$, then it divides $n = X + 10a_1 + a_0$. □

Proof of the rule for 3. We want to show that

$$3 \text{ divides } n \iff 3 \text{ divides } a_k + \cdots + a_1 + a_0.$$

We need to deal with the coefficients 10^j. Note that $10^j = 1 + 3X_j$, where $X_j \in \mathbf{N}$ has j digits, all 3's. So we can expand

$$n = (1 + X_k)a_k + \cdots + (1 + X_1)a_1 + a_0 = X + a_k + \cdots + a_1 + a_0,$$

where $X = X_k a_k + \cdots + X_1 a_1$ is divisible by 3. The rest is the same as the previous proof. □

These proofs are cumbersome. It would be better to avoid carrying around extra variables. As with well-ordering, the key idea to improvement is that we gain power by working with sets rather than their elements.

4.4. *Congruence* First, we say that integers a and b are *congruent modulo* m, and write $a \equiv b \pmod{m}$, if and only if n divides $a - b$.

This is an example of an equivalence relation: That is, we can prove:

(1) $a \equiv a \pmod{m}$.
(2) $a \equiv b \pmod{m}$ if and only if $b \equiv a \pmod{m}$.
(3) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ together imply $a \equiv c \pmod{m}$.

4.5. *Congruence classes* If a is fixed, then the set of all numbers congruent to a mod m is called the *congruence class of a mod m*. Using the definitions, you can check that it is the same set as

$$a + m\mathbf{Z} := \{a + km \mid k \in \mathbf{Z}\}.$$

At this point, we arrive at a subtle yet powerful distinction. I'll illustrate with a specific use case:

Example 4.1. To calculate the congruence class of $6! = 6(5)(4)(3)(2)(1)$ mod 7, we could calculate $6!$ first, then throw in the $7\mathbf{Z}$.

But there is a multiplication operation on congruence classes themselves:

$$\begin{aligned}
&(a + m\mathbf{Z})(b + m\mathbf{Z}) \\
&:= \{(a + jm)(b + km) \mid j, k \in \mathbf{Z}\} \\
&= \{ab + akm + jbm + jkm^2 \mid j, k \in \mathbf{Z}\} \\
&\subseteq \{ab + \ell m \mid \ell \in \mathbf{Z}\} && (\ell = ak + jb + jkm) \\
&=: ab + m\mathbf{Z}.
\end{aligned}$$

So we may as well work at the level of the congruence classes. In particular, we can keep reducing the terms in our work to their (respective) remainders mod 7 before doing further operations, since these remainders are just different representatives of the same congruence classes. We get

$$6! \equiv 30(12)(2) \overset{!}{\equiv} 2(5)(2) \equiv 10(2) \overset{!}{\equiv} 3(2) \equiv 6 \pmod{7}.$$

(The superscripts ! indicate the reductions to remainders.)

4.6. This also works for calculating the congruence class of a sum, because

$$\begin{aligned}
&(a + m\mathbf{Z}) + (b + m\mathbf{Z}) \\
&:= \{(a + jm) + (b + km) \mid j, k \in \mathbf{Z}\} \\
&= \{a + b + \ell m \mid \ell \in \mathbf{Z}\} && (\ell = j + k) \\
&=: (a + b) + m\mathbf{Z}.
\end{aligned}$$

Example 4.2. To calculate $1 + 2 + \cdots + 99 \pmod{7}$, we know that we only need to keep track of the last digit of each summand:

$$\begin{aligned}
1 + 2 + \cdots + 99 &\equiv (1 + 99) + (2 + 98) + \cdots + (49 + 51) + 50 \\
&\equiv \overbrace{100 + 100 + \cdots + 100}^{49 \text{ times}} + 50 \\
&\equiv 2(49) + 1 \pmod{7}.
\end{aligned}$$

But 7 divides 49, so

$$2(49) + 1 \equiv 2(0) + 1 \equiv 1 \pmod{7}.$$

4.7. Useful to introduce the notation:

$$\begin{aligned}\mathbf{Z}/m\mathbf{Z} &:= \{\text{congruence classes modulo } m\} \\ &= \{a + m\mathbf{Z} \mid a \in \mathbf{Z}\} \\ &= \{0 + m\mathbf{Z}, 1 + m\mathbf{Z}, \ldots, (m-1) + m\mathbf{Z}\}.\end{aligned}$$

4.8. I claim that 1 000 002 cannot be a perfect square. Why?

5. 2/15

5.1. Last time we introduced $\mathbf{Z}/m\mathbf{Z}$, the set of congruence classes mod m. We showed that the addition and multiplication of integers descends to addition and multiplication of congruence classes.

Multiplication is the more interesting operation. Here are the multiplication tables for $\mathbf{Z}/5\mathbf{Z}$ and $\mathbf{Z}/6\mathbf{Z}$:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(Above, "a" is an abbreviation for the congruence class $a + m\mathbf{Z}$.) What patterns do you notice? Qualitatively, how are the tables different?

5.2. To me, the most striking thing is that some of the rows/columns list all the elements of $\mathbf{Z}/m\mathbf{Z}$, while others only list a strict subset.

In the table for $\mathbf{Z}/5\mathbf{Z}$, every row/column indexed by a nonzero class is of the first kind. In the table for $\mathbf{Z}/6\mathbf{Z}$, only the rows/columns indexed by 1 or 5 have this property. For example, if $n \in \mathbf{Z}$ is fixed, then

$$2x \equiv n \pmod 5$$

always has a solution for x, but

$$2x \equiv n \pmod 6$$

either has no solutions or multiple solutions.

How can we reliably solve the first congruence for x? We know from the table that $3(2) \equiv 1 \pmod 5$. Therefore $x \equiv 3(2x) \equiv 3n \pmod 5$.

As for the second: Solutions exist only when $n \equiv 0, 2, 4 \pmod 6$: that is, when $n \in 2\mathbf{Z}$. In each case, there are two solutions mod 6. To build intuition, consider a similar example with bigger numbers:

$$12x \equiv n \pmod{20}.$$

This has solutions only when $n \equiv 0, 4, 8, 12, 16 \pmod{20}$: that is, when $n \in 4\mathbf{Z}$. In each case, there are four solutions mod 20.

5.3. Let's gather our observations into formal statements.

Theorem 5.1. *Fix $m \in \mathbf{N}$ and $a, n \in \mathbf{Z}$. Then:*

$$ax \equiv n \pmod m \quad \textit{can be solved for } x \iff n \in \gcd(a, m)\mathbf{Z}.$$

Proof. This is just a reformulation of our earlier theorem about linear Diophantine equations. Indeed,

$$\begin{aligned} & ax \equiv n \pmod{m} \quad \text{can be solved for } x \\ \iff & ax - n = my \text{ can be solved for some } x, y \in \mathbf{Z} \\ \iff & ax + (-m)y = n \text{ can be solved for some } x, y \in \mathbf{Z} \\ \iff & n \in \gcd(a, -m)\mathbf{Z}, \end{aligned}$$

and we know $\gcd(a, -m) = \gcd(a, m)$. □

Theorem 5.2. *In Theorem 5.1, if a and m are coprime, then there is exactly one solution for x mod m.*

Proof. Suppose we have x, x' such that $ax \equiv ax' \equiv n \pmod{m}$. We want to show that $x \equiv x' \pmod{m}$.

Since $\gcd(a, m) = 1$, the previous theorem shows that we can solve $ab \equiv 1 \pmod{m}$ for b. Of course, this also means $ba \equiv 1 \pmod{m}$. Now, we have $x \equiv bax \equiv bax' \equiv x' \pmod{m}$. □

Theorem 5.3. *In Theorem 5.1, the general number of solutions mod m equals* $\gcd(a, m)$.

Proof. We will reduce to the previous theorem. Let $d = \gcd(a, m)$. Let $a' = a/d$ and $m' = m/d$. We claim that if $ax \equiv n \pmod{m}$ has a solution, then d divides n. Indeed, some $x, y \in \mathbf{Z}$ must solve $ax - n = my$, in which case $n = ax - my = d(ax - m'y) \in d\mathbf{Z}$.

Therefore, $n' := n/d$ is an integer. Moreover,

$$(x, y) \text{ solves } ax - n = my \iff (x, y) \text{ solves } a'x - n' = m'y,$$

as we see from dividing through by d. But on the RHS, $\gcd(a', m') = 1$. So the solutions for x on the RHS all belong to the same congruence class mod m'. There are precisely d congruence classes mod m that are contained in a fixed congruence class mod $m' = m/d$. □

Example 5.4. To solve $12x \equiv 8 \pmod{20}$, we first compute $\gcd(12, 20) = 4$. In the notation above, $a' = 12/4 = 3$ and $m' = 20/4 = 5$ and $n' = 8/4 = 2$. The solution to the congruence $3x \equiv 2 \pmod{5}$ is $x \equiv -1 \pmod{5}$. The congruence classes mod 20 that are contained in $-1 + 5\mathbf{Z}$ are

$$-1 + 20\mathbf{Z}, \quad 4 + 20\mathbf{Z}, \quad 9 + 20\mathbf{Z}, \quad 14 + 20\mathbf{Z}.$$

(Note that $19 \equiv 1 \pmod{20}$.) So the solutions to the original congruence are $x \equiv -1, 4, 9, 14 \pmod{20}$.

5.4. *Invertibility* We have seen that if $\gcd(a, m) = 1$, then we can solve $ax \equiv 1 \pmod{m}$ for x. In this case, we say that a is *invertible* modulo m, or a *unit* modulo m.

Note that the solution for x is unique modulo m. We say that x is the *multiplicative inverse* of a modulo m, and write a^{-1} in place of x. In spite of the notation, remember that $a^{-1} \in \mathbf{Z}/m\mathbf{Z}$: It is very different from the fraction $\frac{1}{a} \in \mathbf{Q}$.

We write $(\mathbf{Z}/m\mathbf{Z})^\times$ for the set of invertible congruence classes mod m. Thus

$$(\mathbf{Z}/5\mathbf{Z})^\times = \{1 + 5\mathbf{Z}, 2 + 5\mathbf{Z}, 3 + 5\mathbf{Z}, 4 + 5\mathbf{Z}\},$$
$$(\mathbf{Z}/6\mathbf{Z})^\times = \{1 + 6\mathbf{Z}, 5 + 6\mathbf{Z}\}.$$

One of our observations about the multiplication tables can now be written as:

Theorem 5.5. *Fix $m \in \mathbf{N}$ and $a \in \mathbf{Z}$. The subset*

$$\{ax + m\mathbf{Z} \mid x \in \mathbf{Z}\} \subseteq \mathbf{Z}/m\mathbf{Z}$$

is all of $\mathbf{Z}/m\mathbf{Z}$ when a is invertible mod m, and a strict subset otherwise.

5.5. *Theorems of Fermat and Wilson* Special things happen when the modulus m is prime. Note that if p is prime and $a \notin p\mathbf{Z}$, then a is always coprime to p.

Corollary 5.6 (Fermat's Little Theorem)**.** *If p is prime and does not divide $a \in \mathbf{Z}$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Since $a \notin p\mathbf{Z}$, Theorem 5.5 shows that the sequence $0, a, \ldots, a(p-1)$ mod p is just a reshuffling of the sequence $0, 1, \ldots, (p-1)$ mod p. Therefore, after we exclude the 0 in both lists,

$$a \cdot a(2) \cdots a(p-1) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

But the LHS can be rearranged into $a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \pmod{p}$. Since each of $1, 2, \ldots, (p-1)$ is invertible mod p, we can cancel those terms from both sides, leaving $a^{p-1} \equiv 1 \pmod{p}$. □

What is the value of $(p-1)! \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$, anyway? In lieu of a complete proof, we demonstrate how it works in an example.

Example 5.7. Take $p = 7$. Then the inverses of $1, 2, 3, 4, 5, 6 \pmod 7$ are, respectively, $1, 4, 5, 2, 3, 6 \pmod 7$. We see that 1 and 6 are the only numbers that get paired up with themselves, *i.e.*, form their own inverses. The rest will cancel out with their inverses in the product $6! = 1 \cdot 2 \cdots 6$. We're left with $6! \equiv 1 \cdot 6 \equiv -1 \pmod 7$.

The statement for a general prime p is that $(p-1)! \equiv -1 \pmod{p}$. This is called Wilson's theorem.

6. 2/17

6.1. A quick reminder: Problem Set 2 has been posted, and is due on 2/27. Also, we do have class on the Tuesday after Presidents' Day (2/21), following schoolwide policy.

6.2. Today is devoted to numerical examples. To start off, can we compute $3^{10\,000} \pmod{17}$?

Last time, we covered Fermat's Little Theorem: If $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$. Since 17 is prime, we can apply this theorem to see that $3^{16} \equiv 1 \pmod{17}$. Now observe that $10\,000 = 10^4 = 2^4 5^4$. Therefore,

$$3^{10\,000} = (3^{16})^{5^4} \equiv 1^{5^4} \equiv 1 \pmod{17}.$$

This perhaps illustrates the power of the abstraction we've been discussing.

6.3. If you didn't know about Fermat's theorem, then you might attack the problem by blindly computing powers of 3 mod 17, hoping for a pattern. This will, in fact, work. But it turns out to take 16 steps anyway:

$$\begin{array}{rcccccccccc} n = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots \\ 3^n \equiv & 3 & 9 & 10 & 13 & 5 & 15 & 11 & -1 & \cdots \end{array}$$

I claim that at this point, we immediately know the powers $3^9, 3^{10}, \ldots, 3^{16}$ as well. Indeed, $3^{8+k} \equiv 3^8 3^k \equiv -3^k \pmod{17}$, from which:

$$\begin{array}{rcccccccccc} n = & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & \cdots \\ 3^n \equiv & -3 & -9 & -10 & -13 & -5 & -15 & -11 & 1 & \cdots \end{array}$$

In particular, although the powers of 3 start repeating past $3^{16} \equiv 1$, they do not start repeating at any earlier point. That is, in this example, Fermat's exponent $p - 1$ is a "tight" lower bound for how high you need to go.

6.4. The tables above tell us a lot of other information. For example, since $3^4 \equiv 13$, we immediately know that

$$13^2 \equiv -1, \qquad 13^3 \equiv -13, \qquad 13^4 \equiv 1.$$

In particular, the powers of 13 repeat with period of length 4. Similarly, the powers of 9 repeat with period 8, and the powers of 8 repeat with period 2.

6.5. I claim that you can also read off inverses from these tables very quickly. Recall that the multiplicative inverse of a, if it exists, is the unique value of a^{-1} such that $aa^{-1} \equiv a^{-1}a \equiv 1$.

In our example, we see that we can always find some k such that $a \equiv 3^k$. But we know $3^{16} \equiv 1$, so we must have $a^{-1} \equiv 3^{16-k}$.

For instance, if $a = 11$, then writing $11 \equiv 3^7$ shows that $a^{-1} \equiv 3^{16-7} \equiv 3^9 \equiv -3$. We can check that this is right by computing:

$$11(-3) \equiv -33 \equiv 1 - 34 \equiv 1 \pmod{17}.$$

If instead $a = 12$, then writing $12 \equiv -5 \equiv 3^{13}$ shows that $a^{-1} \equiv 3^{16-13} \equiv 3^3 \equiv 10$.

6.6. *Primitive roots* We've shown how useful it is to know that every nonzero congruence class mod 17 is some power of (the congruence class of) 3. We turn this property into a definition:

An invertible congruence class modulo m is a *primitive root* iff every invertible congruence class modulo m is some power of it. Informally, we say that 3 is a primitive root mod 17. (In this informal language, we would say that -14 and 20 are also primitive roots mod 17.) A useful observation is:

Lemma 6.1. *Suppose p is prime and $a \not\equiv 0 \pmod{p}$. Then a is a primitive root if and only if $a, a^2, \ldots, a^{p-1}$ are pairwise distinct mod p.*

Proof. By definition, a is a primitive root mod p if and only if each invertible congruence class mod p is some power of $a + p\mathbf{Z}$. Since p is prime, there are $p-1$ such classes. At the same time, by Fermat, every power of a is congruent to one of the $p-1$ powers $a, a^2, \ldots, a^{p-1}$. So by the pigeonhole principle, the property holds if and only if that set of powers is exactly the set of invertible classes, which in turn happens if and only if they're pairwise distinct. □

Example 6.2. Take $p = 7$. We see that the powers of 2 mod 7 repeat after $2, 4, 1$, so this can't be a primitive root mod 7. On the other hand, the powers of 3 only repeat after $3, 2, 6, 4, 5, 1$, so we deduce that 3 is a primitive root mod 7, just as it is mod 17.

Note that we could be certain it was primitive after checking up to $3^3 \equiv 6 \equiv -1$: Apply the same reasoning as we used in the mod-17 situation.

Also note that 3 is not the only primitive root mod 7 or 17. For instance, since 5 is the inverse of 3 mod 7, we know that 5 is also a primitive root mod 7: In order, its powers are $5, 4, 6, 2, 3, 1$. This is essentially the sequence of powers of 3 in reverse. Similarly, $-11 \equiv 6$ is the inverse of 3 mod 17, so we know that 6 is also a primitive root mod 17.

However, in the mod-17 setting, there are more options. I claim that $3^7 \equiv 11$ is also a primitive root. Indeed, our table of the powers of 3 shows (together with Fermat) that

$$3^n \equiv 1 \pmod{17} \iff 16 \text{ divides } n.$$

Since $16 = 2^4$ and 2 does not divide 7, we see that

$$(3^7)^n \equiv 1 \pmod{17} \iff 16 \text{ divides } 7n \iff 16 \text{ divides } n.$$

In fact, the primitive roots mod 17 are precisely (the congruence classes of) 3^k for any k coprime to 16, which we may take in the interval $0 \le k < 16$. Can you list all the primitive roots mod 7?

6.7. If the modulus m is composite, then $(\mathbf{Z}/m\mathbf{Z})^\times$ will contain fewer than $m-1$ elements, and we need to be more careful.

Example 6.3. Take $m = 12$. We see that $(\mathbf{Z}/12\mathbf{Z})^\times$ consists of the classes of $1, 5, 7, 11$. But $5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{4}$. So we can't write any of $5, 7, 11$ as a power of either of the other two: There are no primitive roots mod 12.