2.5 Congruences

For this section, we think of m as a fixed positive integer.

Definition 15. We say that a is *congruent* to b modulo m, and we write

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

if m divides $(a - b)$.

IMPORTANT NOTE: All the following statements are equivalent:

- $a \equiv b \pmod{m}$
- a and b give the same remainder when divided by m
- a can be written as $b + km$ for some integer k
- a can be reached from b (and vice versa) by jumping only jumps of length m
- $(a - b)$ is an element of the ideal $\langle m \rangle$

Switching between these different formulations will help you solve most problems concerning congruence questions.

Theorem 12. The relation $a \equiv b \pmod{m}$ is an equivalence relation on $\mathbb{Z}$.

Proof. This should be obvious from the 2nd point above. □

Congruence behave in many ways just like equality. This is very useful in arguments with congruences. To be precise, the following rules hold. (The proofs of these rules is not the important thing, the important thing is that you can use the rules in calculations and arguments.)

Theorem 13 (Rules for congruences)**.** If we have two congruences mod m, we may add them, multiply them, and subtract them. In other words, suppose that

$$a \equiv b \pmod{m} \qquad \text{and} \qquad c \equiv d \pmod{m}$$

Then the following holds:

$$\begin{aligned} a + c &\equiv b + d \pmod{m} \\ ac &\equiv bd \pmod{m} \\ a - c &\equiv b - d \pmod{m} \end{aligned}$$

Proof. Our hypothesis is that m divides $(a - b)$ and m also divides $(c - d)$. Then m must divide $(a - b) + (c - d) = (a + c) - (b + d)$, which gives the first congruence. Similar easy arguments prove the second and third congruence. □

Theorem 14 (More rules for congruences)**.** We may multiply both sides of a congruence by an integer, and we may raise both sides of a congruence to a power. More precisely, suppose that $a \equiv b \pmod{m}$. Then the following holds:

$$na \equiv nb \pmod{m}$$

for every integer n, and

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

for every positive integer n.

Proof. This follows from the previous theorem. Add the congruence $a \equiv b \pmod{m}$ to itself n times to get the $na \equiv nb \pmod{m}$, and multiply it n times to get $a^n \equiv b^n \pmod{m}$. □

Theorem 15 (Cancellation law)**.** If $ac \equiv bc \pmod{m}$ and $GCD(m, c) = 1$, then $a \equiv b \pmod{m}$.

Proof. The first part of the hypothesis says that $m|(ac - bc)$, that is, m divides $c(a - b)$. Since the second part of the hypothesis says that m has no prime factor in common with c, we can conclude that m must divide $(a - b)$. □

Let us now prove a few simple theorems, to show how congruences can be used. The important thing in these examples is not the statement of the theorem, but the method of proof, using congruences.

Theorem 16. Every odd square gives the remainder 1 when divided by 4.

Proof. (Recall that a square is an integer of the form n^2 for some n. Hence the odd squares are 1, 9, 25, 49 and so on.) If a square n^2 is odd, then clearly the number n must also be odd. This implies that n gives remainder 1 or 3 when divided by 4. We consider each of these cases.

Case of remainder 1

In this case, we have

$$n \equiv 1 \pmod{4}$$

Squaring both sides gives

$$n^2 \equiv 1 \pmod{4}$$

which means that n^2 gives remainder 1 when divided by 4.

Case of remainder 3

In this case, we have

$$n \equiv 3 \pmod{4}$$

Squaring both sides gives

$$n^2 \equiv 9 \pmod{4}$$

and since $9 \equiv 1 \pmod{4}$ we have $n^2 \equiv 1 \pmod{4}$. □

As another illustration of the use of congruences, we prove the following fact:

Theorem 17. Let n be a positive integer. Then 3 divides the sum of the digits of n if and only if 3 divides n.

Proof. Suppose that the digits of n are $a_k a_{k-1} \dots a_1 a_0$, where $0 \leq a_j \leq 9$ for each j. (For example, if $n = 924$, then $a_2 = 9$, $a_1 = 2$ and $a_0 = 4$.) Since n is written in base 10, this means that

$$n = \sum_{j=0}^{k} a_j \cdot 10^j = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$$

Of course, the digit sum of n is the number

$$\sum_{j=0}^{k} a_j$$

The crucial step of the proof is to observe the following:

$$a_j \cdot 10^j \equiv a_j \pmod 3 \tag{1}$$

To prove the congruence (1), we can take the congruence

$$10 \equiv 1 \pmod 3$$

and raise each side to the power j, and then multiply both sides by a_j. Now we take the congruence (1) and sum it over all j. This gives us

$$\sum_{j=0}^{k} a_j \cdot 10^j \equiv \sum_{j=0}^{k} a_j \pmod 3$$

This is the same as

$$n \equiv \sum_{j=0}^{k} a_j \pmod 3$$

which means that n is congruent to the digit sum of n, mod 3. This implies that n is divisible by 3 if and only if its digit sum is divisible by 3. □

Now let us prove two important theorems about existence of solutions to certain congruences.

Theorem 18. Let a, b be two integers. Consider the congruence

$$ax \equiv b \pmod m$$

This congruence is solvable (i.e. their exists an integer x satisfying the congruence) if and only if b is a multiple of $GCD(a, m)$.

Proof. First we assume that their exists an x satisfying the congruence. Then $(b - ax)$ is a multiple of m. This implies

$$b - ax = km$$

for some integer k. This implies $b = ax + km$, so b is a linear combination of m and a. Hence $b \in \langle a, m \rangle$, which implies that b is a multiple of $GCD(a, m)$. Now we have to prove the converse. Assume that b is a multiple of $GCD(a, m)$. Then $b \in \langle a, m \rangle$, so

$$b = ax + my$$

for some integers x and y. For this particular x, we see that $b - ax$ is a multiple of m, so x satisfies the congruence of the theorem. □

Theorem 19 (Chinese remainder theorem)**.** Let $a, b \in \mathbb{Z}$, and let m and n be positive coprime integers. Then there exists $z \in \mathbb{Z}$ such that

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

Proof. Since n and m are coprime, we have $\langle m, n \rangle = \mathbb{Z}$. In other words, every integer is a linear combination of m and n. Hence there are some integers x and y such that

$$a - b = xm + yn$$

Now let $z = a - xm$. This implies $z = b + yn$. Now it is obvious that z satisfies the two congruences in the theorem. □

The last theorem of this section is a useful fact about primes.

Theorem 20. A prime $p > 3$ gives remainder 1 or 5 when divided by 6.

Proof. If we divide an integer by 6, the remainder is 0, 1, 2, 3, 4, or 5. Suppose p is prime and greater than 3. Clearly p cannot be even, so the remainder of p when divided by 6 cannot be 0, 2, or 4. Also, the remainder cannot be 3, since this would imply that p is divisible by 3, and hence not prime. Therefore the remainder must be 1 or 5. □

2.5.1 Exercises

For each of the statements E155 to E169, determine whether it is true or false:
E155 $3 \equiv -3 \pmod{5}$
E156 $12 \equiv 24 \pmod{24}$
E157 $0 \equiv 0 \pmod{8}$
E158 $9 \equiv 30 \pmod{7}$

E159 $31 \equiv -26 \pmod 5$
E160 $6 \equiv 132 \pmod{12}$
E161 Every integer n can be written either as $2k$ or as $2k+1$ for some integer k.
E162 If $n \equiv 3 \pmod 5$, then $n^3 \equiv 4 \pmod 5$.
E163 If $a \equiv b \pmod{16}$, then $a \equiv b \pmod 8$.
E164 If $a \equiv b \pmod 5$, then $a \equiv b \pmod{10}$.
E165 If $a \equiv b \pmod m$, then $-a \equiv -b \pmod m$.
E166 If $x \equiv 3 \pmod m$, then $x + 4 \equiv 7 \pmod m$.
E167 If $a \equiv b \pmod m$, then $a^2 \equiv b^3 \pmod m$.
E168 If $2x \equiv 6 \pmod 4$, then $x \equiv 3 \pmod 4$.
E169 If $3a \equiv 3b \pmod 7$, then $a \equiv b \pmod 7$.
E170 What remainders can you get when dividing a square by 3?
E171 What remainders can you get when dividing a square by 5?
E172 Is the congruence $2x \equiv 7 \pmod 3$ solvable? If yes, can you find such an x?
E173 Is the congruence $8x \equiv 6 \pmod{12}$ solvable? If yes, can you find such an x?
E174 Is the congruence $9x \equiv 2 \pmod 6$ solvable? If yes, can you find such an x?
E175 Is the congruence $3x \equiv 5 \pmod 8$ solvable? If yes, can you find such an x?
E176 Is there an integer which gives the remainder 2 when divided by 5 and the remainder 3 when divided by 7? If yes, find such an integer.
E177 Is there an integer which gives the remainder 1 when divided by 10 and the remainder 8 when divided by 9? If yes, find such an integer.
E178 Is there an integer which gives the remainder 2 when divided by 6 and the remainder 3 when divided by 4? If yes, find such an integer.

2.5.2 Problems

P10 Find all prime numbers such that $p^2 + 2$ is also a prime number.
P11 Let n be a positive integer. Prove that n is congruent to the alternating digit sum of n, mod 11.
P12 Prove that if $p > 3$ is a prime, then $24|(p^2 - 1)$.
P13 Find an integer x such that $38x \equiv 5 \pmod{17}$.
P14 Is there a positive integer n such that

$$n^2 \equiv n \pmod p$$

for every prime number p?

2.6 Induction proofs

An important method of proof, which is useful both in number theory and in many other parts of mathematics, is the method of *induction*. It can often be used to prove that a certain statement holds for all positive integers n. Let $S(n)$ denote a statement about the integer n. For example, $S(n)$ could be any of the following statements:

- n is a prime number
- $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$
- $(5^{2n-1} + 1)$ is divisible by 6
- $(n^2 + n + 17)$ is a prime number
- A set with n elements has 2^n subsets
- n can be written as the sum of at most three prime numbers

Consider the first of these examples. In this case, $S(2)$ is a true statement, while $S(4)$ is a false statement. What do you think about the other statements? Are they true for all positive integers n, or only for some positive integers n, or perhaps false for all positive integers n?
If a statement is true for all positive integers n, one way of proving it might be by induction. The idea of an induction proof is the following: Let $S(n)$ be the statement to be proved for all positive integers n.

1. Prove that $S(1)$ is true (Base step)
2. Prove that $S(n)$ implies $S(n+1)$ (Induction step)

If we can prove both of these steps, we may conclude that $S(n)$ is true for all positive integers n (this is called the Principle of Induction).
In most cases, the base step is the easy part and the induction step is the complicated part. However, you must never forget to do both steps, otherwise the proof is not valid! Let us now prove a few theorems to show how induction proofs work.

Theorem 21. For all positive integers n, the integer $(5^{2n-1} + 1)$ is divisible by 6.

Proof. We proceed by induction. The statement $S(n)$ is the statement of the theorem.
Base step: We compute, for $n = 1$:

$$5^{2n-1} + 1 = 6$$

The statement $S(1)$ therefore says that 6 is divisible by 6, which is of course true.
Induction step: Assume that $S(n)$ is true. The statement $S(n+1)$, that we must prove, says the following:

$5^{2(n+1)-1} + 1$ is divisible by 6.

Since $2(n+1) - 1$ is equal to $(2n+1)$, we must prove that

$5^{2n+1} + 1$ is divisible by 6.

How can be prove this? We must use the statement $S(n)$, which we assume to be true. Reformulating in terms of congruences, $S(n)$ says that

$$5^{2n-1} \equiv -1 \pmod 6$$

Multiplying both sides by 25, we get

$$5^{2n+1} \equiv -25 \pmod 6$$

and since $-25 \equiv -1 \pmod 6$, we can conclude that

$$5^{2n+1} \equiv -1 \pmod 6$$

which implies that $S(n+1)$ is true.
By the Principle of Induction we now know that $S(n)$ is true for all positive integers n. □

Theorem 22. Let n be a positive integer. The sum of the first n positive integers is equal to $\frac{n(n+1)}{2}$.

Proof. The statement $S(n)$ to be proved is the following statement:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

The statement $S(n+1)$ is the following:

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$$

Let's proceed by induction.
Base step: Consider the statement $S(n)$ for $n = 1$. In this case, we have

$$\sum_{k=1}^{n} k = 1$$

and

$$\frac{n(n+1)}{2} = 1$$

so the statement $S(1)$ is true.
Induction step: Assume that the statement $S(n)$ is true. We must use this to prove $S(n+1)$. The statement $S(n)$ says

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Now add $(n+1)$ to both sides of this equality. We get

$$\big(\sum_{k=1}^{n} k\big) + (n+1) = \frac{n(n+1)}{2} + (n+1)$$

which is the same as

$$\sum_{k=1}^{n+1} k = \frac{n^2}{2} + \frac{n}{2} + n + 1$$

But the right hand side of this equality is equal to $\frac{(n+1)(n+2)}{2}$ (check this!) which means that we have proved the statement $S(n+1)$.
Now the Principle of Induction allows us to conclude that $S(n)$ is true for all n. □

Theorem 23. If A is a set with n elements, then A has 2^n subsets.

Proof. Recall that we proved the following lemma in the lectures (we omit this proof here, as the important point is the induction proof):

Lemma 1. Let the finite set A have one more element than the set B. Then A has twice as many subsets as B.

Let us now the induction proof. The statement $S(n)$ is the statement of the theorem.
Base step: The statement $S(1)$ is true, because a set A with one element has exactly two subsets: the empty set and the set A itself.
Induction step: Assume that $S(n)$ is true. This means that a set with n elements has 2^n subsets. By the lemma we can see that a set with $(n+1)$ elements has $2 \cdot 2^n$ subsets, that is 2^{n+1} subsets. Hence the statement $S(n+1)$ is also true.
Now the Principle of Induction allows us to conclude that $S(n)$ is true for all positive integers n. □

Let us again summarize the method of induction:

- In the base step, we prove that $S(1)$ is true
- In the induction step, we *assume* that $S(n)$ is true, and use this to prove that $S(n+1)$ is true

2.6.1 Exercises

E179 Prove that $2^{3n} \equiv 1 \pmod 7$ for every positive integer n.
E180 Prove that $3^n \equiv 3 \pmod 6$ for every positive integer n.

2.6.2 Problems

P15 Try to find a formula for the sum of the first n odd numbers.

For the last two problems, we define the *Fibonacci numbers* as follows:

$$\begin{aligned} F_1 &= 1 \\ F_2 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \qquad \text{for } n \geq 2 \end{aligned}$$

We can easily compute $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$ and so on.
P16 Prove that F_{3n} is even for every n. (In other words, prove that F_3, F_6, F_9 and so on are all even.)
P17 Prove that

$$F_n F_{n+2} + (-1)^n = F_{n+1}^2$$

for all positive integers n.

2.7 The Euler φ function

In general, a function defined on the positive integers (i.e. with $\mathbb{Z}^+$ as the domain) is usually called an *arithmetic function*. There are many interesting and useful arithmetic functions, but in this course we shall only have time to look at one.

Definition 16. For any positive integer n, we define $\varphi(n)$ to be the number of elements in the set $\{1, 2, \ldots, n\}$ that are coprime to n.

Example 32. Among the numbers 1, 2, 3, 4, only the number 1 and 3 are coprime to 4. Hence $\varphi(4) = 2$.

Example 33. Among the numbers 1, 2, 3, 4, 5, 6, 7, every number except 7 is coprime to 7. Hence $\varphi(7) = 6$.

Theorem 24. If the prime factorization of n is $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then the following formula holds:

$$\varphi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Proof. Omitted. □

We will not need the above general formula (and you don't have to remember it for the exam), but we shall need the following two special cases (which you must remember).

Corollary 1. If p is a prime number, then $\varphi(p) = p - 1$. If p and q are prime numbers, and $n = pq$, then $\varphi(n) = (p-1)(q-1)$.

Proof. This follows from the general formula. □

Example 34. Using the corollary, we can compute that

$$\begin{aligned} \varphi(11) &= 10 \\ \varphi(29) &= 28 \\ \varphi(15) &= 2 \cdot 4 = 8 \\ \varphi(35) &= 24 \\ \varphi(22) &= 10 \end{aligned}$$

Theorem 25 (Euler's theorem)**.** Let $n \geq 2$ be an integer, and let a be a positive integer coprime to n. Then the following congruence holds:

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

Proof. This will be proved later, using a general theorem in group theory. □

Theorem 26 (Fermat's little theorem)**.** If p is a prime number, and a is a positive integer, then

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

Proof. We consider two cases.
Case 1: p divides a.
In this case, $a \equiv 0 \pmod{p}$. Hence $a^p \equiv 0 \pmod{p}$, so the theorem is true in this case.
Case 2: p does not divide a.
We know that $\phi(p) = p - 1$. Since a is coprime to p, we may apply Euler's theorem (with $n = p$) to get the following congruence:

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

Multiplying both sides by a proves the theorem also in the second case. □

Example 35. Fermat's little theorem is of great help when dealing with congruences mod a prime number. Consider for example the following question:

What is the remainder of 4^{22} when divided by 7?

Since 4^{22} is a very large number, the question looks difficult. But Fermat's little theorem tells us that

$$4^7 \equiv 4 \pmod 7$$

Raising both sides to the power 3 gives us

$$4^{21} \equiv 4^3 \pmod 7$$

and multiplying both sides by 4 gives

$$4^{22} \equiv 4^4 \pmod 7$$

Since $4^4 = 256$, and the number 256 gives remainder 4 when divided by 7, we can conclude that 4^{22} also gives remainder 4.

2.7.1 Exercises

Compute the following, using either the definition of φ or the general formula:
E181 $\varphi(16)$
E182 $\varphi(77)$
E183 $\varphi(12)$
E184 $\varphi(21)$
E185 $\varphi(39)$
E186 $\varphi(19)$
E187 Prove that $2^{62} \equiv 4 \pmod{77}$.
E188 Prove that $8^{25} \equiv 8 \pmod{39}$.
E189 Prove that $(5^{21} - 125)$ is a multiple of 19.
E190 Prove that if p is a prime number, then

$$a^{p^2} \equiv a \pmod p$$

for every positive integer a.
E191 Find the remainder when 6^{89} is divided by 11.
E192 Find the last digit of the integer 7^{401}.
E193 Find the remainder when $3 \cdot (5^{56})$ is divided by 8.

2.7.2 Problems

P18 Let a and b be positive integers, and let p be a prime number. Prove that

$$(a+b)^p \equiv a^p + b^p \pmod p$$

P19 Let p be an odd prime number. Prove that the sum

$$1^p + 2^p + \ldots + (p-1)^p$$

is divisible by p.