

These notes and problems are intended to review the number theoretic material we have covered so far. The problems mostly involve directly applying the definition of congruences, and the various algorithms we have learned (Euclidean algorithm, extended Euclidean algorithm). There is also a problem on the Chinese Remainder Theorem and a problem that asks us to find primitive roots for a certain prime modulus. Finally, I prove and go over Fermat's Little Theorem and Euler's Theorem. In general, we should be able to understand these proofs and have an idea of how to construct such proofs on our own.

Theorem 1. *If $x_1 \equiv y_1 \pmod{n}$ and $x_2 \equiv y_2 \pmod{n}$, then $x_1 \pm x_2 \equiv y_1 \pm y_2 \pmod{n}$ and $x_1 \cdot x_2 \equiv y_1 \cdot y_2 \pmod{n}$.*

Proof. If $x_1 \equiv y_1 \pmod{n}$, we know we can write $x_1 = y_1 + kn$ for some $k \in \mathbb{Z}$. Likewise, we can write $x_2 = y_2 + ln$ for some $l \in \mathbb{Z}$. Adding or subtracting these values will give us $x_1 \pm x_2 = y_1 \pm y_2 + (k \pm l)n$. Since k and l are both integers, we know that $k \pm l$ will also be an integer, so in particular we still have an integer multiple of n . Reducing this equation modulo n will therefore give us $x_1 \pm x_2 \equiv y_1 \pm y_2 \pmod{n}$. For multiplication, we keep the same equations as above and compute $x_1 \cdot x_2 = (y_1 + kn)(y_2 + ln) = y_1y_2 + (ky_2 + ly_1)n + kln^2$. By the same reasoning that told us $k \pm l \in \mathbb{Z}$, we can see that $ky_2 + ly_1 \in \mathbb{Z}$ and $kln \in \mathbb{Z}$, so we again have integer multiples of n . Reducing modulo n , we find that $x_1 \cdot x_2 \equiv y_1 \cdot y_2 \pmod{n}$. \square

The previous problem really was just a direct application of the idea of a congruence; if you had any trouble with it you should definitely review what a congruence means and the various operations you can perform within a certain modulus. Next, we explore the Euclidean algorithm and the extended Euclidean algorithm.

Theorem 2. *The inverse of 11 modulo 41 is 15, that is $11 \cdot 15 \equiv 1 \pmod{41}$.*

Proof. Using the Euclidean Algorithm, we find

$$\begin{aligned} 41 &= 3(11) + 8 \\ 11 &= 8 + 3 \\ 8 &= 2(3) + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Now, working backwards with the Extended Euclidean Algorithm, we get

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 2 \cdot 3) = 3(3) - 8 \\ &= 3(11 - 8) - 8 = 3(11) - 4(8) \\ &= 3(11) - 4(41 - 3 \cdot 11) = 15(11) - 4(41) \end{aligned}$$

Therefore, we have $1 = 15(11) - 4(41)$, which we can reduce modulo 41 to see that $15 \cdot 11 \equiv 1 \pmod{41}$. \square

The next problem involves the Chinese Remainder Theorem. The method used here is different from the method used in Shoup and the one that many of you used on your homeworks, but try to understand it and use whichever one is more intuitive.

Theorem 3. *The set of congruences*

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

has the set of solutions $x \equiv 23 \pmod{105}$ and in particular the smallest solution $x = 23$.

Proof. To start, we write $x = 2 + 3k$ for some $k \in \mathbb{Z}$. Then we can plug this into our next congruence to see that $2 + 3k \equiv 3 \pmod{5}$, $3k \equiv 1 \pmod{5}$. Now we need to compute the inverse of 3 modulo 5, which even just by guessing we can see is 2 (since $3 \cdot 2 = 6 \equiv 1 \pmod{5}$). So, $k \equiv 2 \pmod{5}$, which tells us that $k = 2 + 5l$ for some $l \in \mathbb{Z}$. We can plug this information into our equation for x to see that $x = 2 + 3k = 2 + 3(2 + 5l) = 8 + 15l$. Note that we have now solved our congruences for the first two, and we can simply repeat the process with this answer and our last congruence to get the answer for all three congruences. So, we plug in $8 + 15l \equiv 2 \pmod{7}$, $15l \equiv -6 \equiv 1 \pmod{7}$. Since $15 \equiv 1 \pmod{7}$, we actually have that $l \equiv 1 \pmod{7}$, so this time we don't even need to find an inverse. We now have that $l = 1 + 7m$, which we plug into our equation for x to see that

$$x = 8 + 15l = 8 + 15(1 + 7m) = 23 + 105m$$

To get the smallest solution, we simply take $m = 0$ to see that $x = 23$. In general, however, we reduce modulo 105 to see that $x \equiv 23 \pmod{105}$. \square

The next problem involves primitive roots, which we hopefully remember from class. Although we may not use primitive roots much, they are actually quite powerful and have a lot of uses in cryptography. For more information, feel free to ask me!

Theorem 4. *If we test the numbers 2, 3, 4, and 5 to see if they are primitive roots modulo 7, we find that 3 and 5 are, but 2 and 4 are not.*

Proof. To start, we recall that a primitive root for a given modulus p (also known as a generator) is an integer g such that $\langle g \rangle = (g, g^2, g^3, \dots) = \mathbb{Z}_p^*$. In other words, the different powers of g modulo p will give us all the different elements. Another way of stating this is that $p-1$ is the smallest value x such that $g^x \equiv 1 \pmod{p}$. Starting with 2, we see that $\langle 2 \rangle = (2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8 \equiv 1, \dots)$. At this point, we can actually stop calculating values, because we know that once we have reached 1, we have hit all the possible values (since then we'll have $2^4 \equiv 2$, $2^5 \equiv 4$, and so on; remember that these groups are cyclic). Since $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ and $\langle 2 \rangle = \{1, 2, 4\}$, we can see that 2 is not a primitive root. Moving on to 3, we have $\langle 3 \rangle = (3, 2, 6, 4, 5, 1, \dots)$. Therefore, 3 must be a primitive root. For 4 and 5, we have $\langle 4 \rangle = (4, 2, 1, \dots)$ and $\langle 5 \rangle = (5, 4, 6, 2, 3, 1, \dots)$, which tells us that 5 is a primitive root modulo 7, while 4 is not. \square

Hopefully this problem has illustrated that finding primitive roots is not particularly easy (i.e. there is no way to find them other than trying one at a time). We can therefore view them as a sort of “trapdoor”; if you know the primitive root for a prime p you can compute things about \mathbb{Z}_p^* that would otherwise be hard. Now, we get into some slightly more advanced theorems about congruences. Note that there is a fair amount of number theory background that we are just assuming for now (but as always, if you want to know more, ask me!).

Theorem 5 (Lemma). *If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. Assume that $p \nmid a$. Then, by the definition of a prime, we know that a and p must be relatively prime, so by the extended Euclidean algorithm there exist integers k and l such that $ak + lp = 1$. We can multiply this equation through by b to see that $abk + lpb = b$. We see that p clearly divides the left-hand side of this equation, since $p \mid p$ by definition and $p \mid ab$ by assumption. Therefore, it must also divide the right-hand side, which tells us that $p \mid b$. \square

Theorem 6 (Fermat’s Little Theorem). *For p a prime, we have that for all $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. To start, we proved in the last homework that multiplication by a given element in \mathbb{Z}_p^* is a permutation on \mathbb{Z}_p^* , that is it will just return all the elements of \mathbb{Z}_p^* in a different order. Therefore, we can say that

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

Now, we note that we have multiplied a $p-1$ times and that we can pull out the factors of a to get

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

Since every element of \mathbb{Z}_p^* is relatively prime to p , we can use the lemma to see that the product of any two elements of \mathbb{Z}_p^* is also relatively prime to p . In fact, we can extend this idea inductively to see that a product of any number of elements of \mathbb{Z}_p^* is relatively prime to p . In particular, the product of ALL the elements of the group is relatively prime to p . Therefore, we know that the product $1 \cdot 2 \cdot \dots \cdot (p-1)$ must have some inverse modulo p , and that we can multiply both sides of our congruence by this multiplicative inverse to effectively cancel and get that $a^{p-1} \equiv 1 \pmod{p}$. \square

Now, we can look at a theorem known as Euler’s Theorem, which just generalizes Fermat’s Little Theorem to the case when p is not necessarily a prime. The proof is almost identical, so see if you can do it yourself!

Theorem 7 (Euler’s Theorem). *For n an integer and all $a \in \mathbb{Z}_n^*$, we have $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n) = \{0 < x < n : \gcd(x, n) = 1\}$ (this is known as Euler’s totient function).*

Proof. To start, we recall that the size of \mathbb{Z}_n^* is $|\mathbb{Z}_n^*| = \phi(n)$. Therefore, we can label the elements of the group as $\{b_1, b_2, \dots, b_{\phi(n)}\}$. We have seen that multiplication by a given element in \mathbb{Z}_n^* is a permutation on \mathbb{Z}_n^* . So, we can say that for $a \in \mathbb{Z}_n^*$:

$$(a \cdot b_1)(a \cdot b_2) \dots (a b_{\phi(n)}) \equiv b_1 \cdot b_2 \cdot \dots \cdot b_{\phi(n)} \pmod{p}.$$

Now, we note that we have multiplied a exactly $\phi(n)$ times and that we can pull out the factors of a to get

$$a^{\phi(n)}(b_1 \cdot b_2 \cdot \dots \cdot b_{\phi(n)}) \equiv b_1 \cdot b_2 \cdot \dots \cdot b_{\phi(n)} \pmod{p}.$$

Since every element of \mathbb{Z}_n^* is relatively prime to n , we can use the lemma to see that the product of any two elements of \mathbb{Z}_n^* is also relatively prime to n . In fact, we can extend this idea inductively to see that a product of any number of elements of \mathbb{Z}_n^* is relatively prime to n . In particular, the product of ALL the elements of the group is relatively prime to n . Therefore, we know that the product $b_1 \cdot b_2 \cdot \dots \cdot b_{p-1}$ must have some inverse modulo n , and that we can multiply both sides of our congruence by this multiplicative inverse to effectively cancel and get that $a^{\phi(n)} \equiv 1 \pmod{n}$. \square