Due: Saturday, 9/24, 4:00 PM
Grace period until Saturday, 9/24, 6:00 PM

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

I worked on problem 6a with **Sri Chandramouli (sri.c@berkeley.edu)** during an office hours session. I did not work with anybody else.

1 Modular Practice

Solve the following modular arithmetic equations for x and y.

(a) $9x + 5 \equiv 7 \pmod{11}$.

Solution: We can rearrange this to be $9x \equiv -2 \pmod{11}$, which can then be written as $9x \equiv -9 \pmod{11}$ so this implies that $x = -1$. And further, since we can add multiples of 11 without issue (since any multiple of 11 is divisible by 11), then we have the general solution for x: $\forall n \in \mathbb{Z}$, $x = -1 + 11n$

(b) Show that $3x + 15 \equiv 4 \pmod{21}$ does not have a solution.

Solution: This is equivalent to writing $3x \equiv -11 \pmod{21}$ or $3x \equiv 10 \pmod{21}$. To show that this has no solution, we analyze the possible residues of multiples of 3 modulo 21. Any multiple of 3 can only be $3, 6, 9, 12, 15, 18$ modulo 21 (since they're multiples of 3), so since 10 is not on this list, this equation has no solution.

(c) The system of simultaneous equations $3x + 2y \equiv 0 \pmod 7$ and $2x + y \equiv 4 \pmod 7$.

Solution: We can solve this system of equations in the same way we solve any system of equations: multiply the latter equation by 2 to get $4x + 2y \equiv 8 \equiv 1 \pmod 7$

$$3x + 2y - (4x + 2y) \equiv -1 \pmod 7$$

From here we get that $-x \equiv 1 \pmod 7 \implies x = 1 + 7n$ for all $n \in \mathbb{Z}$. Now we can solve for y, by letting $x = 1$ for simplicity:

$$3 + 2y \equiv 0 \pmod{12}$$
$$2y \equiv 5 \pmod{7}$$
$$\therefore y \equiv 2 \pmod{7}$$

This implies the solutions $y = 2 + 7n$ for all $n \in \mathbb{Z}$. Thus, our solutions for x and y are in the form $x = 1 + 7n$ and $y = 2 + 7k$ for all $k, n \in \mathbb{Z}$.

(d) $13^{2019} \equiv x \pmod{12}$.

Solution: Notice that $13 \equiv 1 \pmod{12}$ and so our equation becomes $x \equiv 1^{2019} \pmod{12}$ so therefore the result is 1.

(e) $7^{21} \equiv x \pmod{11}$.

Solution: We can rewrite $7^{21} = \left(7^3\right)^7$ and since $7^3 \equiv 2 \pmod{11}$, which is easily computable. This means that

$$128 \equiv 2 \pmod{11}$$

And since 121 is a power of 11, then the remainder would be 7, which is our answer.

2 Nontrivial Modular Solutions

(a) What are all the possible perfect cubes modulo 7?

Solution: Every perfect cube can be decomposed into $0, 1^3, 2^3, \ldots, 6^3$ when taken modulo 7. Thus, we can construct a chart:

x	$x^3 \pmod 7$
0	0
1	1
2	1
3	-1
4	1
5	-1
6	-1

Therefore all the perfect cubes are $\{-1, 0, 1\}$ modulo 7.

(b) Show that any solution to $a^3 + 2b^3 \equiv 0 \pmod 7$ must satisfy $a \equiv b \equiv 0 \pmod 7$.

Solution: We use the previous part, as well as the additive property of modular arithmetic, except in reverse: if $a^3 \equiv c \pmod 7$ then $2b^3 \equiv -c \pmod 7$, so that the net sum on the right hand side remains zero. Since we've shown that $a^3 \equiv \pm 1$ modulo 7 when $a \not\equiv 0 \pmod 7$, this implies that

$$2b^3 \equiv \pm - 1 \pmod 7$$

But since $b^3 \equiv \pm 1 \pmod 7$, this means that $2b^3 \equiv \pm 2 \pmod 7$, implying that there is no solution to $2b^3 \pm -1 \pmod 7$. Thus, the only solution arises when $c = 0$, which would imply that $a^3 \equiv 0 \pmod 7$ and $2b^3 \equiv 0 \pmod 7$, which gives us $a \equiv b \equiv 0 \pmod 7$.

(c) Using part (b), prove that $a^3 + 2b^3 = 7a^2b$ has no non-trivial solutions (a, b) in the integers. In other words, there are no integers a and b, that satisfy this equation, except the trivial solution $a = b = 0$.

[*Hint:* Consider some nontrivial solution (a, b) with the smallest value for $|a|$ (why are we allowed to consider this?). Then arrive at a contradiction by finding another solution (a', b') with $|a'| < |a|$.]

Solution: We use the hint. Suppose there is a smallest nontrivial solution (a, b) with the smallest value of $|a|$ that satisfies this equation. We know from the previous part that $a \equiv b \equiv 0 \pmod 7$, so thus we can write $a = 7k$ and $b = 7m$ for some $k, m \in \mathbb{Z}$. So we can rewrite the above equation:

$$(7k)^3 + 2(7m)^3 = 7(7k^2)(7m)$$
$$7^3 k^3 + 2 \cdot 7^3 m^3 = 7^4 k^2 m$$
$$\therefore k^3 + 2m^3 = 7k^2 m$$

But this last equation suggests that (k, m) is also a valid solution. And since $a = 7k \implies |k| = |a/7| < |a|$ then this means that this solution pair (k, m) is smaller than our original (a, b). This is a contradiction, since we assumed earlier that (a, b) was the nontrivial pair with the smallest $|a|$. As a result, this equation has no nontrivial solutions (a, b).

It's also easy to show that the trivial solution $(a, b) = (0, 0)$ is valid since both the left and right hand sides equal zero. ∎

3 Wilson's Theorem

Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

Prove both directions (it holds if AND only if p is prime).

Hint for the if direction: Consider rearranging the terms in $(p-1)! = 1 \cdot 2 \cdots \cdots (p-1)$ to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod{q}$?

Solution: For the if case: we attempt to match every number with its multiplicative inverse. Since every number in the set $S = \{1, 2, \ldots, p-1\}$ exists in $(p-1)!$ and they are all relatively prime to p, every number within this set also has a multiplicative inverse modulo p.

However, the multiplicative inverse of $p-1$ and 1 are themselves. Since there is only one copy of $p-1$ and 1 in $(p-1)!$, this means that these are the only two numbers which cannot be multiplied with their multiplicative inverses.

Furthermore, we know that for all other numbers within S its multiplicative inverse also exists in S, since the multiplicative inverse of a number is also coprime to p, and thus also exists within S. Finally, since multiplicative inverses are unique, we know that each integer in S can be paired with a unique number which guarantees that a pairing exists.

Thus, if we take the product of all numbers, we have $\frac{p-1}{2}$ pairs which are all equal to 1 modulo p, so we have:

$$(p-1)! \equiv 1(p-1) \equiv -1 \pmod{p}$$

For the only if direction, we consider the hint. If p is composite, then this means it has some prime factor q, and thus $(p-1)! \equiv 0 \pmod{q}$. Now consider the original statement:

$$(p-1)! \equiv -1 \pmod{p}$$

And rearrange it to

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

If p is composite and $(p-1)! \equiv 0 \pmod{q}$, then this implies that $(p-1)! + 1 \equiv 1 \pmod{q}$. However, we know that $(p-1)! + 1 \equiv 0 \pmod{p}$. This is a contradiction, since q is a prime factor p so any number divisible by p must also be divisible by q, but $(p-1)! + 1 \equiv 1 \pmod{q}$ implies that this expression is *not* divisible by q while being divisible by p. Thus our original statement is incorrect for composite p, so $(p-1)! \not\equiv 0 \pmod{p}$. ∎

4 Fermat's Little Theorem

Without using induction, prove that $\forall n \in \mathbb{N}$, $n^7 - n$ is divisible by 42.

Solution: First, we factor $n^7 - n = n(n^6 - 1)$. Since $42 = 2 \cdot 3 \cdot 7$, this means that if we can show that $n^7 - n$ can be both divisible by 2, 3 and 7 then we are also done. We can also show these independently since 2, 3 and 7 are all prime numbers, so they share no factors besides 1.

First, let's show that $n^7 - n \equiv 0 \pmod 2$. This is easy: if n is even, then $n^7 - n$ is clearly even since the difference of two even numbers is even. Further, if n is odd, then $n^7 - n$ is still even since the difference of two odd numbers is also even.

Now let's show that $n^7 - n \equiv 0 \pmod 3$. Since all residues modulo 3 are either $0, \pm 1$, this means the following:

- If $n \equiv 0 \pmod 3$ then clearly $n^7 - n$ is divisible.

- If $n \equiv 1 \pmod 3$ then $n^7 - n \equiv 1^7 - 1 \equiv 0 \pmod 3$, so this is divisible by 3 as well.

- If $n \equiv -1 \pmod 3$ then $n^7 - n \equiv (-1)^7 + 1 \equiv 0 \pmod 3$, so this is also divisible by 3.

Finally, let's analyze the factorization. If $n \equiv 0 \pmod{42}$ then we are done. Now we look at the case where $n \not\equiv 0 \pmod{42}$. From Fermat's little theorem, we know that $n^6 \equiv 1 \pmod 7$ for all $n \in \{1, 2, \ldots, 6\}$. However, we can extend this further to any n, since the base of the exponential can always be rewritten as a power of $\{1, 2, \ldots, 6\}$ modulo 7. Thus, $n^6 - 1 \equiv 0 \pmod 7$ for any n, and so this is always divisible by 7.

Since this number is always divisible by 2, 3, and 7, then $n^7 - n$ is always divisible by 42 $\forall n \in \mathbb{N}$. ∎

5 Euler's Totient Function

Euler's totient function is defined as follows:

$$\phi(n) = |\{i : 1 \leq i \leq n, \gcd(n,i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than or equal to n which are relatively prime to it. We develop a general formula to compute $\phi(n)$.

(a) Let p be a prime number. What is $\phi(p)$?

Solution: $\phi(p) = p - 1$, since by definition, no number less than p divides p.

(b) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

Solution: The numbers which are not coprime to p^k will be the multiples of p. Since we can write $p^k = p^{k-1} \cdot p$, this means that there are p^{k-1} multiples of p which are less than p^k. Thus, $\phi(p^k) = p^k - p^{k-1}$.

(c) Show that if $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. (Hint: Use the Chinese Remainder Theorem.)

Solution: From the chinese remainder theorem, we know that if

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

Guarantees a unique c which satisfies $x \equiv c \pmod{mn}$. This means that for any (a,b) we choose, there will be a unique value of c. Now consider the following: if x is coprime to m, then it follows from the Euclidean algorithm that $\gcd(x,m) = \gcd(m, x \pmod{m}) = 1$ and since $x \equiv a \pmod{m}$, then this implies that $\gcd(m,a) = 1$. The same argument goes for x and n: $\gcd(x,n) = \gcd(n,b) = 1$. In other words, this means that if x is coprime to m, then a is also coprime to m, and likewise for b and n.

Now, instead of looking for integers which are coprime to m and n, we can now shift our focus to a and b since if x is coprime to m and n this is the same as looking for numbers a and b which are individually coprime to m and n respectively.

For m, there are $\phi(m)$ numbers coprime to m, meaning that there are $\phi(m)$ choices of a we can make. Likewise, there are $\phi(n)$ choices of b that we can make as well. Thus, there are $\phi(m)\phi(n)$ ways of choosing (a,b) such that x is coprime to m and coprime to n.

Finally, notice that if $\gcd(x,m) = \gcd(x,n) = 1$, then it follows that $\gcd(x,mn) = 1$. Had this not been true, then it would mean that x would have shared a factor with either m or n so either $\gcd(x,m) \neq 1$ or $\gcd(x,n) \neq 1$. Thus, becuase this fact is true, then this means that every unique x we found by selecting (a,b) not only corresponds to a unique x, but also an x which is coprime to mn and therefore in $\phi(mn)$. Since a and b can be chosen independently of each

other, this means that for every value of a we choose there are $\phi(n)$ ways of choosing b. Thus, there are $\phi(m)\phi(n)$ total ways of choosing (a,b).

We also need to prove that this list is complete. That is, there doesn't exist an integer $k \in \phi(mn)$ such that it does not appear in $\phi(m)$ or $\phi(n)$. If this is true, then this means that $\gcd(k,m)$ or $\gcd(k,n)$ is not equal to 1, and if this is true then k cannot be coprime to n. ∎

(d) Argue that if the prime factorization of $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then

$$\phi(n) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}$$

Solution: Firstly, notice that since each prime is coprime to the all other primes, we can write

$$\phi(n) = \phi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k})$$
$$= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$$

Now we expand the given product:

$$n \prod_{i=1}^{k} \frac{p_i - 1}{p_i} = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \frac{(p_1 - 1) \cdots (p_k - k)}{p_1 \cdots p_k}$$
$$= p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1)$$
$$= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$$

Since these expressions are the same we are done. ∎

6 Euler's Totient Theorem

Euler's Totient Theorem states that, if n and a are coprime,

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

where $\phi(n)$ (known as Euler's Totient Function) is the number of positive integers less than or equal to n which are coprime to n (including 1).

(a) Let the numbers less than n which are coprime to n be $m_1, m_2, \ldots, m_{\phi(n)}$. Argue that the set

$$\{am_1, am_2, \ldots, am_{\phi(n)}\}$$

is a permutation of the set

$$\{m_1, m_2, \ldots, m_{\phi(n)}\}.$$

In other words, prove that

$$f : \{m_1, m_2, \ldots, m_{\phi(n)}\} \to \{m_1, m_2, \ldots, m_{\phi(n)}\}$$

is a bijection, where $f(x) := ax \pmod{n}$.

Solution: In order to prove that f is a bijection, that is it both injective and surjective. In other words, there is a one-to-one correspondence and that each element in the original set has a corresponding value in the imaged set.

Suppose for the sake of contradiction that the function is not injective. That is, there exist two elements in the original set that map to the same element in the image. Mathematically, this means that there exists m_1, m_2 such that

$$am_1 \equiv am_2 \pmod{n}$$

Since a is coprime to n, we can multiply both sides with its multiplicative inverse (which is the same thing as "dividing" by a) to get:

$$m_1 \equiv m_2 \pmod{n}$$

But this is impossible, since m_1, m_2 are both distinct numbers coprime to n. Thus we've reacehd a contradiction, so f must be surjective.

Now to prove that f is surjective, we choose an element m_i in the set, and prove that we can always find another element m_j within this set which under f maps to m_i. Mathematically, this means

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

In order for this to be true, then $x = a^{-1} m_i$. Since a is coprime to n, then a^{-1} is also coprime to n. Further, the product of two numbers coprime to n must also be coprime to n. Thus, x is coprime to n. If x is larger than n, we can subtract x by n as many times as we like until x is

less than n without altering its coprimality. Thus, if x is now less than n, it must be contained in $\{m_1, \ldots, m_n\}$, since this is the set of numbers coprime to n. Thus, there always exists an x, so f must be injective.

Since we've proved both injectivity and surjectivity for f, f is a bijection on this set, and we are done. ■

(b) Prove Euler's Theorem. (Hint: Recall the FLT proof.)

Solution: We follow in a similar fashion to the FLT proof. Consider the set S to be the numbers coprime to n: $S = \{m_1, m_2, \ldots, m_{\phi(n)}\}$. Now consider $S' = aS = \{am_1, \ldots, am_{\phi(n)}\}$ for some a coprime to n. From part (a) we've shown that when this set is taken modulo n it is a permutation of S, and so S' contains the same elements as S, just in a different order. Since they contain the same elements, the product of elements in S and S' must be the same, so we set them equal to each other:

$$m_1 m_2 \cdots m_{\phi(n)} \equiv a m_1 a m_2 \cdots a m_{\phi(n)} \pmod{n}$$

There are $\phi(n)$ numbers on the right hand side, so we can rewrite the equation as

$$m_1 m_2 \cdots m_{\phi(n)} \equiv a^{\phi(n)} m_1 m_2 \cdots m_{\phi(n)} \pmod{n}$$

Since each of $m_1, m_2, \ldots, m_{\phi(n)}$ are coprime to n, we can multiply both sides by the multiplicative inverse of each m_i to get:

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

Which is precisely what we wanted to prove. ■

7 Sparsity of Primes

A prime power is a number that can be written as p^i for some prime p and some positive integer i. So, $9 = 3^2$ is a prime power, and so is $8 = 2^3$. $42 = 2 \cdot 3 \cdot 7$ is not a prime power.

Prove that for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers.

Hint: This is a Chinese Remainder Theorem problem. We want to find x such that $x+1, x+2, \dots, x+k$ are all not powers of primes. We can enforce this by saying that $x+1$ through $x+k$ each must have two distinct prime divisors.

Solution: We use the Chinese Remainder Theorem in order to solve this. The idea is in order to enforce that $x+1$ through $x+k$ must have two distinct primes, we can choose $2k$ primes $\{p_1, p_2, \dots, p_{2k}\}$ and set up the following list of congruences:

$$
\begin{aligned}
x+1 &\equiv 0 \pmod{p_1 p_2} \\
x+2 &\equiv 0 \pmod{p_3 p_4} \\
&\;\;\vdots \\
x_k &\equiv 0 \pmod{p_{2k-1} p_{2k}}
\end{aligned}
$$

This set guarnatees that each of $x+1$ through $x+k$ is divisible by at least two primes. Rearranging these congruences, we get:

$$
\begin{aligned}
x &\equiv -1 \pmod{p_1 p_2} \\
x &\equiv -2 \pmod{p_3 p_4} \\
&\;\;\vdots \\
x &\equiv -k \pmod{p_{2k-1} p_{2k}}
\end{aligned}
$$

Since $\{p_1, p_2, \dots, p_{2k}\}$ are all distinct primes, then $p_1 p_2, p_3 p_4, \dots p_{2k-1} p_{2k}$ must all be relatively prime to one another. Since they are all coprime, then the Chinese Remainder Theorem tells us that there must exist an x which satisfies all these congruences. Once x is found, then $x+1, \dots, x+k$ is the desired sequence. ∎