CS 70 Discrete Mathematics and Probability Theory
Fall 2022 Satish Rao and Babak Ayazifar

HW 04

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.)

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 withotu 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). 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:

$$\begin{aligned} 3+2y &\equiv 0 \pmod{12} \\ 2y &\equiv 5 \pmod{7} \\ \therefore y &\equiv 2 \pmod{7} \end{aligned}$$

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 $1^{2019} \pmod{12}$ 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

(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. Now let's look at the latter equation. Since we've shown that all nonzero numbers are ± 1 modulo 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 nonzero solution to $2b^3 \pm -1 \pmod 7$ for nonzero c. Thus, the only solution arises when $c = 0$, which would imply that $a^3 \equiv 0 \pmod 7$ and $2b^3 \equiv 0 \pmod 7$, with each equation implying that $a \equiv 0 \pmod 7$ and $b \equiv 0 \pmod 7$, respectively.

(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:

$$\begin{aligned}(7k)^3 + 2(7m)^3 &= 7(7k^2)(7m) \\ 7^3k^3 + 2 \cdot 7^3m^3 &= 7^4k^2m \\ \therefore k^3 + 2m^3 &= 7k^2m\end{aligned}$$

But this last equation seemingly 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 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 solution 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 $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ 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 $(p-1)! \pmod{q}$?

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 that will not be coprime to p^k will be $p, p^2, \ldots, p^k$. There are k numbers here, so $\phi(p^k) = p^k - k$.

(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. Since the number of ways we can do this is $\phi(m)\phi(n)$, this means that $\phi(mn) = \phi(m)\phi(n)$.

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

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

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 $f(x) \coloneqq ax \pmod{n}$.

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

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 $x+1, x+2, \ldots, x+k$ 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: Apologies in advance because my solution is not the intended one.

We prove that $k!+1, k!+2, \ldots, k!+k$ can be chosen as the consecutive positive integers for $k \geq 4$, and we show that consecutive integers also exist for $k < 4$ by example. Let's do the example first, to get it out of the way. If $k = 1$, 15 is a solution. If $k = 2$, the numbers $15, 16$ are a valid pair. If $k = 3$, then $14, 15, 16$ is a valid triplet. Now we prove this is true for $k \geq 4$.

Let's look at the string of k integers again. Notice that for any $a \leq k$, we can rewrite the term $k!+a$ in the following way:

$$k! + a = a\left(\frac{k!}{a} + 1\right)$$

$k!/a$ is guaranteed to be divisible by a, since $a \leq k$, so $k!$ contains a as a factor. Now we need to prove that $k!+a$ is not a prime power for any $a < k$. Notice that in order for $k!+a$ to be a prime power, then it follows that $k!/a+1$ must also be a prime power, since a prime power can only be expressed as a product of two smaller prime powers.[1] Now notice that

$$\frac{k!}{a} + 1 \equiv 1 \pmod{a}$$

So this term can never be a prime power. And since this works for any $a < k$, none of the integers in $k!+1, \ldots, k!+k$ can be prime powers, so we are done. ■

[1] We can prove this is true by noticing that for any b given prime a:

$$a^n b = a^m \implies b = \frac{a^m}{a^n} = a^{m-n}$$

which is clearly a prime power.