CS 70 Discrete Mathematics and Probability Theory
Fall 2025 Sabin, Hug

HW 04

1 Modular Practice

Note 6

Solve the following modular arithmetic equations for x and y. For each subpart, show your work and justify your answers.

(a) $9x+5 \equiv 7 \pmod{13}$.

(b) Prove that $3x+12 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $5x+4y \equiv 0 \pmod{7}$ and $2x+y \equiv 4 \pmod{7}$.

(d) $13^{2023} \equiv x \pmod{12}$.

(e) $7^{62} \equiv x \pmod{11}$.

Solution:

(a) Subtract 5 from both sides to get:

$$9x \equiv 2 \pmod{13}.$$

Now since $\gcd(9,13) = 1$, 9 has a (unique) inverse mod 13, and since $9 \times 3 = 27 \equiv 1 \pmod{13}$ the inverse is 3. So multiply both sides by $9^{-1} \equiv 3 \pmod{13}$ to get:

$$x \equiv 6 \pmod{13}.$$

(b) Notice that any number $y \equiv 4 \pmod{21}$ can be written as $y = 4+21k$ (for some integer k). Evaluating y mod 3, we get $y \equiv 1 \pmod{3}$.

Since the right side of the equation is $1 \pmod{3}$, the left side must be as well. However, $3x+12$ will never be $1 \pmod{3}$ for any value of x. Thus, there is no possible solution.

(c) First, subtract the first equation from four times the second equation to get:

$$\begin{aligned} 4(2x+y)-(5x+4y) &\equiv 4(4)-0 \pmod{7} \\ 8x+4y-5x-4y &\equiv 16 \pmod{7} \\ 3x &\equiv 2 \pmod{7} \end{aligned}$$

Multiplying by $3^{-1} \equiv 5 \pmod{7}$, we have $x \equiv 10 \equiv 3 \pmod{7}$.

Plugging this into the second equation, we have

$$2(3)+y \equiv 4 \pmod{7},$$

so the system has the solution $x \equiv 3 \pmod{7}$, $y \equiv 5 \pmod{7}$.

(d) We use the fact that $13 \equiv 1 \pmod{12}$. Thus, we can rewrite the equation as

$$x \equiv 13^{2023} \equiv 1^{2023} \equiv 1 \pmod{12}.$$

(e) One way to solve exponentiation problems is to test values until one identifies a pattern.

$$\begin{aligned}
7^1 &\equiv 7 \pmod{11} \\
7^2 &\equiv 49 \equiv 5 \pmod{11} \\
7^3 &= 7 \cdot 7^2 \equiv 7 \cdot 5 \equiv 2 \pmod{11} \\
7^4 &= 7 \cdot 7^3 \equiv 7 \cdot 2 \equiv 3 \pmod{11} \\
7^5 &= 7 \cdot 7^4 \equiv 7 \cdot 3 \equiv 10 \equiv -1 \pmod{11}
\end{aligned}$$

We theoretically could continue this until we the sequence starts repeating. However, notice that if $7^5 \equiv -1 \implies 7^{10} = (7^5)^2 \equiv (-1)^2 \equiv 1 \pmod{11}$.

Similarly, $7^{60} = (7^{10})^6 \equiv 1^6 \equiv 1 \pmod{11}$. As a final step, we have $7^{62} = 7^2 \cdot 7^{60} \equiv 7^2 \cdot 1 = 49 \equiv 5 \pmod{11}$.

2 Short Answer: Modular Arithmetic

Note 6

For each subpart, show your work and justify your answers.

(a) What is the multiplicative inverse of $n-1$ modulo n? (Your answer should be an expression that may involve n)

(b) What is the solution to the equation $3x \equiv 6 \pmod{17}$?

(c) Let $R_0 = 0; R_1 = 2; R_n = 4R_{n-1} - 3R_{n-2}$ for $n \geq 2$. Is $R_n \equiv 2 \pmod{3}$ for $n \geq 1$? (True or False)

(d) Given that $(7)(53) - m = 1$, what is the solution to $53x + 3 \equiv 10 \pmod{m}$? (Answer should be an expression that is interpreted $\pmod{m}$, and shouldn't consist of fractions.)

Solution:

(a) The answer is $n-1 \pmod{n}$. We can see this by noting that it is $-1 \pmod{n}$, or more directly, $(n-1)(n-1) \equiv n^2 - 2n + 1 \equiv 1 \pmod{n}$.

(b) The answer is $x \equiv 2 \pmod{17}$. Muliply both sides by 6 (the multiplicative inverse of 3 modulo 17) and reduce.

(c) The statement is true. We can see this by taking the recursive formula modulo 3. This gives us that $R_n \equiv R_{n-1} \pmod{3}$, hence since $R_1 \equiv 2 \pmod{3}$, every R_i must also be 2 modulo 3.

(d) Note that since $7 \cdot 53 - m = 1$, we can take both sides modulo m and find that $7 \cdot 53 \equiv 1 \pmod{m}$, hence 7 is the inverse of 53 modulo m. Thus, we can solve the equation by subtracting by 3 on both sides and multiplying by 7, giving that $x \equiv 49 \pmod{m}$.

3 Wilson's Theorem

Note 6

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 $(p-1)! \pmod{q}$?

Solution:

Direction 1: If p is prime, then the statement holds.

For the integers $1, \cdots, p-1$, every number has an inverse. However, it is not possible to pair a number off with its inverse when it is its own inverse. This happens when $x^2 \equiv 1 \pmod{p}$, or when $p \mid x^2 - 1 = (x-1)(x+1)$. Thus, $p \mid x-1$ or $p \mid x+1$, so $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. Thus, the only integers from 1 to $p-1$ inclusive whose inverse is the same as itself are 1 and $p-1$.

We reconsider the product $(p-1)! = 1 \cdot 2 \cdots p-1$. The product consists of 1, $p-1$, and pairs of numbers with their inverse, of which there are $\frac{p-1-2}{2} = \frac{p-3}{2}$. The product of the pairs is 1 (since the product of a number with its inverse is 1), so the product $(p-1)! \equiv 1 \cdot (p-1) \cdot 1 \equiv -1 \pmod{p}$, as desired.

Direction 2: The expression holds *only if* p is prime (contrapositive: if p isn't prime, then it doesn't hold).

We will prove by contradiction that if some number p is composite, then $(p-1)! \not\equiv -1 \pmod{p}$. Suppose for contradiction that $(p-1)! \equiv -1 \pmod{p}$. Note that this means we can write $(p-1)!$ as $p \cdot k - 1$ for some integer k.

Since p isn't prime, it has some prime factor q where $2 \leq q \leq n-2$, and we can write $p = q \cdot r$. Plug this into the expression for $(p-1)!$ above, yielding us $(p-1)! = (q \cdot r)k - 1 = q(rk) - 1 \implies (p-1)! \equiv -1 \pmod{q}$. However, we know q is a term in $(p-1)!$, so $(p-1)! \equiv 0 \pmod{q}$. Since $0 \not\equiv -1 \pmod{q}$, we have reached our contradiction.

4 Celebrate and Remember Textiles

Note 6

You've decided to knit a 70-themed baby blanket as a gift for your cousin and want to incorporate rows from three different stitch patterns with the following requirements on the row lengths of each of the stitch patterns:

- Alternating Link: Multiple of 8, plus 3
- Double Helix: Multiple of 3, plus 1

- Crossover: Multiple of 7, plus 6

You want to be able to switch between knitting these different patterns without changing the number of stitches on the needle, so you must use a number of stitches that simultaneously meets the requirements of all three patterns.

Find the *smallest number of stitches* you need to cast on in order to incorporate all three patterns in your baby blanket.

Solution: Let x be the number of stitches we need to cast on. Using the Chinese Remainder Theorem, we can write the following system of congruences:

$$\begin{aligned} x &\equiv 3 \pmod 8 \\ x &\equiv 1 \pmod 3 \\ x &\equiv 6 \pmod 7. \end{aligned}$$

We have $M = 8 \cdot 3 \cdot 7 = 168$, $r_1 = 3, m_1 = 8, b_1 = M/m_1 = 3 \cdot 7 = 21$, $r_2 = 1, m_2 = 3, b_2 = M/m_2 = 8 \cdot 7 = 56$, and $r_3 = 6$, $m_3 = 7$, $b_3 = M/m_3 = 8 \cdot 3 = 24$. We need to solve for the multiplicative inverse of b_i modulo m_i for $i \in \{1,2,3\}$:

$$\begin{aligned} b_1 a_1 &\equiv 1 \pmod{m_1} \\ 21 a_1 &\equiv 1 \pmod 8 \\ 5 a_1 &\equiv 1 \pmod 8 \\ \rightarrow a_1 &= 5, \end{aligned}$$

$$\begin{aligned} b_2 a_2 &\equiv 1 \pmod{m_2} \\ 56 a_2 &\equiv 1 \pmod 3 \\ 2 a_2 &\equiv 1 \pmod 3 \\ \rightarrow a_2 &= 2, \end{aligned}$$

and

$$\begin{aligned} b_3 a_3 &\equiv 1 \pmod{m_3} \\ 24 a_3 &\equiv 1 \pmod 7 \\ 3 a_3 &\equiv 1 \pmod 7 \\ \rightarrow a_3 &= 5. \end{aligned}$$

Therefore,

$$\begin{aligned} x &\equiv 3 \cdot 21 \cdot 5 + 1 \cdot 56 \cdot 2 + 6 \cdot 24 \cdot 5 \pmod{168} \\ &\equiv 1147 \equiv 139 \pmod{168}, \end{aligned}$$

so the smallest x that satisfies all three congruences is 139. Therefore we should cast on 139 stitches in order to be able to knit all three patterns into the blanket.

5 Sparsity of Primes

Note 6

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 n such that $(n+1)$, $(n+2)$, $\ldots$, and $(n+k)$ are all not powers of primes. We can enforce this by saying that $n+1$ through $n+k$ each must have two distinct prime divisors. In your proof, you can choose these prime divisors arbitrarily.

Solution:

We want to find n such that $n+1, n+2, n+3, \ldots, n+k$ are all not powers of primes. We can enforce this by saying that $n+1$ through $n+k$ each must have two distinct prime divisors. So, select $2k$ primes, $p_1, p_2, \ldots, p_{2k}$, and enforce the constraints

$$\begin{aligned}
n+1 &\equiv 0 \pmod{p_1 p_2} \\
n+2 &\equiv 0 \pmod{p_3 p_4} \\
&\vdots \\
n+i &\equiv 0 \pmod{p_{2i-1} p_{2i}} \\
&\vdots \\
n+k &\equiv 0 \pmod{p_{2k-1} p_{2k}}.
\end{aligned}$$

By Chinese Remainder Theorem, we can calculate the value of n, so this n must exist, and thus, $n+1$ through $n+k$ are not prime powers.

What's even more interesting here is that we could select any $2k$ primes we want!