CS 70 Discrete Mathematics and Probability Theory
Fall 2023 Rao, Tal

HW 04

1 Modular Practice

Note 6

Solve the following modular arithmetic equations for x and y.

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

(b) Show 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 Nontrivial Modular Solutions

Note 6

(a) What are all the possible perfect cubes modulo 7? In other words, compute the set

$$\{x^3 \bmod 7 \mid x \in \mathbb{Z}\}.$$

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

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

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

Solution:

(a) Checking by hand, the only perfect cubes modulo 7 are 0, 1, and $6 \equiv -1$:

$$\begin{array}{ll}
0^3 \equiv 0 \pmod 7 & 4^3 \equiv 1 \pmod 7 \\
1^3 \equiv 1 \pmod 7 & 5^3 \equiv -1 \pmod 7 \\
2^3 \equiv 1 \pmod 7 & 6^3 \equiv -1 \pmod 7 \\
3^3 \equiv -1 \pmod 7 &
\end{array}$$

(b) Considering the equation $x^3 + 2y^3 \equiv 0 \pmod 7$ and considering all cases for x^3 and y^3, the only way that $x^3 + 2y^3 \equiv 0 \pmod 7$ is if $x^3 \equiv y^3 \equiv 0 \pmod 7$. Thus $x \equiv y \equiv 0 \pmod 7$.

(c) We first show that if (x,y) is a solution to $x^3+2y^3=7x^2y$, then $x=0$ implies that $y=0$. In other words, if $x=0$, then the solution must be trivial. To see why this is the case, suppose that $x=0$. Then $y^3=0$, and so $y=0$. Thus, any nontrivial solution must have $x \neq 0$, or equivalently, $|x|>0$.

If (x,y) is a solution to the original equation, then this is also a solution to

$$x^3+2y^3 \equiv 0 \pmod{7}.$$

From part (b), we know that x,y are all divisible by 7, which in turn means that x^3, y^3 are divisible by 7^3. Thus, we can divide the entire original equation by 7^3, to see that

$$\left(\frac{x}{7}\right)^3+2\left(\frac{y}{7}\right)^3=7\left(\frac{x}{7}\right)^2\left(\frac{y}{7}\right).$$

Indeed, $(x/7, y/7)$ is another solution where all the values are integers, and $|x/7|<|x|$ (as $|x|>0$). We've reached a contradiction to our initial assumption, which was that (x,y) was the solution with the least value of $|x|$. (This is a valid assumption since the $|x|$ are positive integers, and a non-empty set of positive integers has a minimum.) Thus, there does not exist a nontrivial solution to $x^3+2y^3=7x^2y$.

3 Squares

Note 6
Note 7

Let p be a prime greater than 2. We will prove that there exists an integer a such that $a^2 \equiv -1 \pmod{p}$ if and only if $p \equiv 1 \pmod{4}$.

(a) Show that if $p \equiv 3 \pmod{4}$, there is no integer a such that $a^2 \equiv -1 \pmod{p}$. (Hint: Use Fermat's Little Theorem.)

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

(c) Show that if $p \equiv 1 \pmod{4}$, there is an integer a such that $a^2 \equiv -1 \pmod{p}$. (Hint: Consider $a = \left(\frac{p-1}{2}\right)!$, then use Wilson's Theorem.)

Solution:

(a) Suppose for the sake of a contradiction that there exists a solution a. First, note that $a \equiv 0 \pmod{p}$ is not a solution. Now, suppose $a \not\equiv 0 \pmod{p}$. Raise both sides to the $\frac{p-1}{2}$ power. Since $p \equiv 3 \pmod{4}$, $\frac{p-1}{2}$ is an odd integer. Thus, we have that

$$1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

since -1 to an odd integer is -1. Thus, we have that $p \mid 1-(-1) = 2$, which is not possible, since $p \equiv 3 \pmod{4}$. Thus, there is no solution to $a^2 \equiv -1 \pmod{p}$, as desired.

(b) *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.

(c) Since p is odd, $\frac{p-1}{2}$ is an integer, so $\left(\frac{p-1}{2}\right)!$ exists. Our goal here is to try to connect $\left(\frac{p-1}{2}\right)!^2$ to $(p-1)!$, in order to utilize Wilson's theorem; if we can show that $\left(\frac{p-1}{2}\right)!^2 \equiv (p-1)! \pmod{p}$, then Wilson's theorem will directly give us the desired result.

Notice that we can express

$$\left(\frac{p-1}{2}\right)!^2 \equiv \left(1 \cdot 2 \cdots \frac{p-3}{2} \cdot \frac{p-1}{2}\right) \cdot \left(\frac{p-1}{2} \cdot \frac{p-3}{2} \cdots 2 \cdot 1\right) \pmod{p}$$

Now, if we can turn the second half of the expansion into the terms $\frac{p+1}{2}$, $\frac{p+3}{2}$, $\ldots$, $(p-1)$, then the entire expansion will equal $(p-1)!$; to do this, we can negate each term in the second half of the expansion. Further, since $p \equiv 1 \pmod 4$, we know that $\frac{p-1}{2}$ is even, so we've introduced an even number of factors of -1, and these negations will all cancel out. Using this and simplifying, we have

$$\begin{aligned}
&\equiv \left(1\cdot 2\cdots \frac{p-3}{2}\cdot\frac{p-1}{2}\right)\cdot\left(\left(-\frac{p-1}{2}\right)\cdot\left(-\frac{p-3}{2}\right)\cdots(-2)\cdot(-1)\right) \pmod p\\
&\equiv \left(1\cdot 2\cdots \frac{p-3}{2}\cdot\frac{p-1}{2}\right)\cdot\left(\left(p-\frac{p-1}{2}\right)\cdot\left(p-\frac{p-3}{2}\right)\cdots(p-1)\right) \pmod p\\
&\equiv \left(1\cdot 2\cdots \frac{p-3}{2}\cdot\frac{p-1}{2}\right)\cdot\left(\frac{p+1}{2}\cdot\frac{p+3}{2}\cdots(p-1)\right) \pmod p\\
&\equiv (p-1)! \pmod p\\
&\equiv -1 \pmod p
\end{aligned}$$

where in the last line we applied Wilson's Theorem. As such, we can conclude that

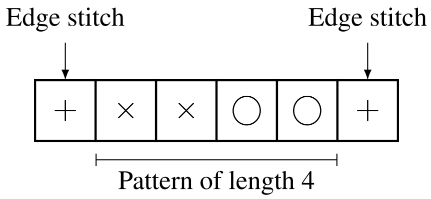
$$\left(\frac{p-1}{2}\right)!^2 \equiv -1 \pmod p,$$

as desired.

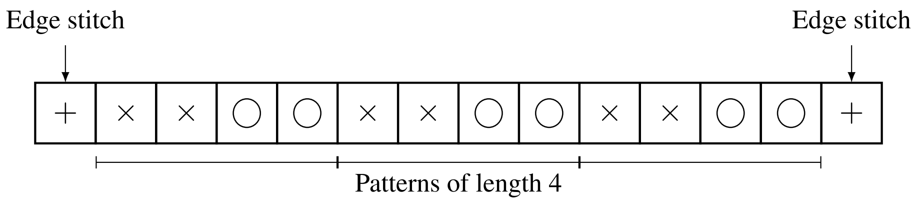
4 Celebrate and Remember Textiles

Note 6 Mathematics and computing both owe an immense debt to textiles, where many key ideas originated.

Instructions for knitting patterns will tell you to begin by "casting on" the needle some multiple of m plus r, where m is the number of stitches to create one repetition of the pattern and r is the number of stitches needed for the two edges of the piece. For example, in the simple rib stitch pattern below, the repeating pattern is of length $m = 4$, and you need $r = 2$ stitches for the edges.



Thus, to make the final piece wider, you can add as many multiples of the pattern of length 4 as you like; for example, if you want to repeat the pattern 3 times, you need to cast on a total of $3m + r = 3(4) + 2 = 14$ stitches (shown below).



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:

- Alternating Link: Multiple of 7, plus 4
- Double Broken Rib: Multiple of 4, plus 2
- Swag: Multiple of 5, plus 2

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:

$$\begin{aligned} x &\equiv 4 \pmod{7} \\ x &\equiv 2 \pmod{4} \\ x &\equiv 2 \pmod{5}. \end{aligned}$$

We have $M = 7 \cdot 4 \cdot 5 = 140$, $r_1 = 4$, $m_1 = 7$, $b_1 = M/m_1 = 4 \cdot 5 = 20$, $r_2 = 3$, $m_2 = 4$, $b_2 = M/m_2 = 7 \cdot 5 = 35$, and $r_3 = 2$, $m_3 = 5$, $b_3 = M/m_3 = 7 \cdot 4 = 28$. We need to solve for the multiplicative inverse of b_i modulo m_i for $i \in \{1,2,3\}$:

$$\begin{aligned} b_1 a_1 &\equiv 1 \pmod{m_1} \\ 20a_1 &\equiv 1 \pmod{7} \\ 6a_1 &\equiv 1 \pmod{7} \\ \rightarrow a_1 &= 6, \\ \\ b_2 a_2 &\equiv 1 \pmod{m_2} \\ 35a_2 &\equiv 1 \pmod{4} \\ 3a_2 &\equiv 1 \pmod{4} \\ \rightarrow a_2 &= 3, \end{aligned}$$

and

$$\begin{aligned} b_3a_3 &\equiv 1 \pmod{m_3} \\ 28a_3 &\equiv 1 \pmod{5} \\ 3a_3 &\equiv 1 \pmod{5} \\ \to a_3 &= 2. \end{aligned}$$

Therefore,

$$\begin{aligned} x &\equiv 6 \cdot 20 \cdot 4 + 2 \cdot 35 \cdot 3 + 2 \cdot 28 \cdot 2 \pmod{140} \\ &\equiv 102 \pmod{140}, \end{aligned}$$

so the smallest x that satisfies all three congruences is 102. Therefore we should cast on 102 stitches in order to be able to knit all three patterns into the blanket.

5 Euler's Totient Theorem

Note 6
Note 7

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

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

Solution:

(a) This problem mirrors the proof of Fermat's Little Theorem, except now we work with the set $\{m_1, m_2, \cdots, m_{\phi(n)}\}$.

Since m_i and a are both coprime to n, so is $a \cdot m_i$. Suppose $a \cdot m_i$ shared a common factor with n, and WLOG, assume that it is a prime p. Then, either $p|a$ or $p|m_i$. In either case, p is a common factor between n and one of a or m_i, contradiction.

We now prove that f is injective. Suppose we have $f(x) = f(y)$, so $ax \equiv ay \pmod{n}$. Since a has a multiplicative inverse $\pmod{n}$, we see $x \equiv y \pmod{n}$, thus showing that f is injective.

We continue to show that f is surjective. Take any y that is relatively prime to n. Then, we see that $f(a^{-1}y) \equiv y \pmod{n}$, so therefore, there is an x such that $f(x) = y$. Furthermore, $a^{-1}y \pmod{n}$ is relatively prime to n, since we are multiplying two numbers that are relatively prime to n.

(b) Since both sets have the same elements, just in different orders, multiplying them together gives

$$m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)} \equiv am_1 \cdot am_2 \cdot \ldots \cdot am_{\phi(n)} \pmod{n}$$

and factoring out the a terms,

$$m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)} \equiv a^{\phi(n)} \left(m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)}\right) \pmod{n}.$$

Thus we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

6 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.

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!