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

HW 04

Due: Saturday, 9/23, 4:00 PM
Grace period until Saturday, 9/23, 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

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

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 $|x'| < |x|$.]

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

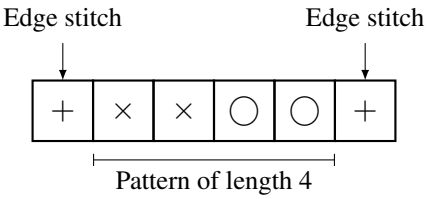
(c) Show that if $p \equiv 1 \pmod{4}$, there is an integer a such that $a^2 \equiv -1 \pmod{p}$. (Hint: Consider $a = \left(\frac{p-1}{2}\right)!$, then use Wilson's Theorem.)

4 Celebrate and Remember Textiles

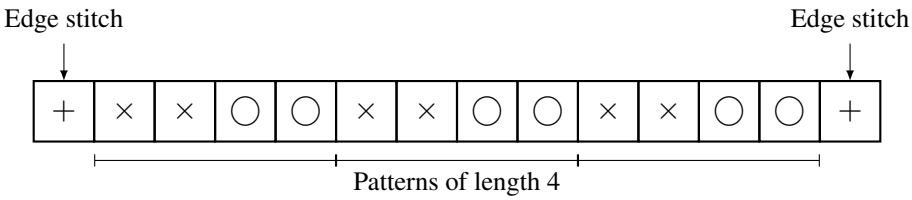
Note 6

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.

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

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

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.*