CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 04

Due: Saturday, 2/17, 4:00 PM
Grace period until Saturday, 2/17, 6:00 PM

Sundry

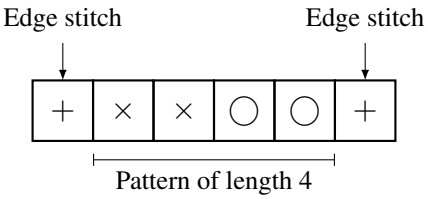
Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Celebrate and Remember Textiles

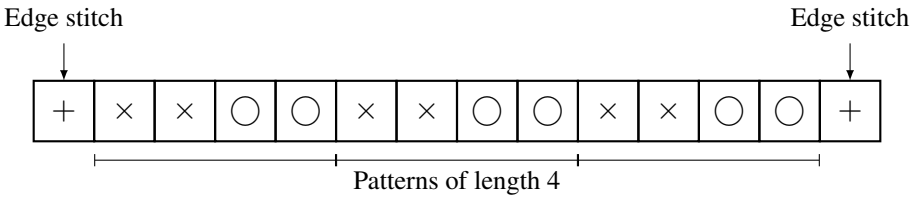
Note 6

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.

2 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). Note that this theorem generalizes Fermat's Little Theorem, since if n is prime, then $\phi(n) = n-1$.

(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.)

3 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.*

1. $x \equiv 4 \pmod 7$
$\equiv 2 \pmod 4$
$\equiv 2 \pmod 5$
$\Rightarrow x \equiv 102 \pmod{140}$

$n+2, n+3, \ldots, n+k$ a

ough $n+k$ each must

enforce the constraints

$$+1 \equiv 0 \pmod{p_1 p_2}$$

$$+2 \equiv 0 \pmod{p_3 p_4}$$

$\vdots$

2 (a) We first note that $\{am \mid \phi(n)\}$ is also coprime to n as a & $m \mid \phi(n)$ are coprime to n

Next, we see that if $am_2 \equiv am_1 \bmod n$ for $1 \neq 2$

multiply both sides by a^{-1} (exist because coprime)

$a^{-1}am_2 \equiv a^{-1}am_1 \Rightarrow m_2 \equiv m_1 \bmod n$

which is impossible. Thus $\{am\}$ all different

Thus as $\{am\}$ are coprime and different by pigeon hole principle, they must be permutation of $\{n\}$

(b) by (a), $\prod am \equiv \prod m \equiv a^{\phi(n)} \prod m \equiv \prod m \bmod n$

as $\prod m$ coprime with n, it has inverse

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

Q, $a \equiv a^{1+\phi(n)}$

$a \equiv a^{-2}$?

$a \equiv a^{-3}$?

3 We know that the number of prime integers approach $\frac{n}{\ln n}$

We also note that the span of each prime power for individual prime grows exponentially, for example $2^1 \cdot 2^1 = 2^2$

Simply put, the next prime power would be multiple distance of the prior prime power to the n

Thus for n large enough, each prime contributes $1 + \frac{\ln(n-d)}{\ln d}$ prime powers, the density of prime powers are

$\frac{n}{\sum (1 + \frac{\ln(n-d)}{\ln d})} \leq \frac{n}{\sum_{1}^{n} 1} = \ln n$ As $\lim_{n \to \infty} \ln n \to \infty$ Density approaches int

Thus, we can find an interval that satisfy the stem.

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!

Alternative solution.

CRT only requires coprime

4 RSA Practice

Note 7

Consider the following RSA scheme and answer the specified questions.

(a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key d? Calculate the exact value.

(b) If the receiver gets 4, what was the original message?

(c) Encode your answer from part (b) to check its correctness.

5 Tweaking RSA

Note 7

You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

(a) Show how you choose e and d in the encryption and decryption function, respectively. Prove the correctness property: the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve now compute d in the decryption function? If so, by what algorithm?

(c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain the modifications made to encryption and decryption and include a proof of correctness showing that $D(E(x)) = x$.

4.(a) $(p-1)(q-1) = 4 \cdot 10 = 40$

$q^{-1} \pmod{40} = 9$

As $9 \cdot 9 = 81 \bmod 40 = 1$

Thus $d = 9$.

(b) $D(C(E(x))) \equiv E(x)^d \equiv 4^9 \bmod 55$

$\equiv 64^3 \bmod 55 \equiv 9^3 \bmod 55 \equiv 14$

14 is the message

(c) $14^e \bmod 55 \equiv 14^9 \equiv (2744)^3 \equiv (-6)^3 \equiv 4 \bmod 55$

5 (a) d is inverse of e under $p-1$

$x^{de} \equiv x^{kp \cdot v + 1} \equiv x(x^k)^{p-1} \equiv x \bmod p$

by Fermat's little theorem.

(b) γ_{+1} Extended Euclidean.

(c) d = inverse of e under $(q-1)(p-1)(r-1)$

Similarly $x^{de} \equiv x \bmod p, q, r$

Thus by CRT, x unique under p, qr.