1 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 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 $i \in \{1,2,3\}$:

$$\begin{aligned} b_1 a_1 &\equiv 1 \pmod{m_1} \\ 20 a_1 &\equiv 1 \pmod 7 \\ 6 a_1 &\equiv 1 \pmod 7 \\ \rightarrow a_1 &= 6, \end{aligned}$$

$$\begin{aligned} b_2 a_2 &\equiv 1 \pmod{m_2} \\ 35 a_2 &\equiv 1 \pmod 4 \\ 3 a_2 &\equiv 1 \pmod 4 \\ \rightarrow a_2 &= 3, \end{aligned}$$

and

$$
\begin{aligned}
b_3 a_3 &\equiv 1 \pmod{m_3} \\
28 a_3 &\equiv 1 \pmod{5} \\
3 a_3 &\equiv 1 \pmod{5} \\
\to a_3 &= 2.
\end{aligned}
$$

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.

2 Euler's Totient Function

Note 6

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 $\phi(p)$?

(b) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

(c) We want to show that if $\gcd(a,b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$. Let us proceed by direct proof, and assume that $\gcd(a,b) = 1$ for the subparts of this problem.

  (i) Show that for $z \equiv x \pmod{a}$, if $\gcd(x,a) = 1$, then $\gcd(z,a) = 1$.

  (ii) Let X be the set of positive integers $1 \leq i \leq a$ such that $\gcd(i,a) = 1$ (i.e. all numbers in mod a that are coprime to a), and let Y, Z be defined analogously for mod b, ab respectively. Use the Chinese Remainder Theorem to show that there is a bijection between $X \times Y$ and Z.

  (iii) Use the above parts to show that $\phi(ab) = \phi(a)\phi(b)$.

(d) Show that if the prime factorization of $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

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

Solution:

(a) Since p is prime, all the numbers from 1 to $p-1$ are relatively prime to p.

So, $\phi(p) = p-1$.

(b) The only positive integers less than p^k which are not relatively prime to p^k are multiples of p.

Why is this true? This is so because the only possible prime factor which can be shared with p^k is p. Hence, if any number is not relatively prime to p^k, it has to have a prime factor of p which means that it is a multiple of p.

The multiples of p which are $\leq p^k$ are $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$. There are p^{k-1} of these.

The total number of positive integers less than or equal to p^k is p^k.

So $\phi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1)$.

(c) (i) $z = x + ka$ for some integer k. Then, $x = z - ka$. By contraposition, if z and a both have a nonzero common divisor d, then $z - ka$ is also divisible by d, and therefore so is x.

(ii) We will construct a bijective function $f : X \times Y \to Z$. Given (x, y), a tuple from X, Y respectively, we will construct an instance of CRT using the equations

$$
\begin{aligned}
z &\equiv x \pmod{a} \\
z &\equiv y \pmod{b}
\end{aligned}
$$

Since $\gcd(a,b) = 1$, we know that there exists a unique solution $z \pmod{ab}$ to these equations by CRT. As the name suggests, we want to show now that $z \in Z$. Using the previous part, we can conclude that $\gcd(z,a) = 1$ and $\gcd(z,b) = 1$. Since $\gcd(a,b) = 1$, we can conclude that $\gcd(z,ab) = 1$, which indeed shows that $z \in Z$. Since the CRT is bijective, we have therefore established a bijection between $X \times Y$ and Z.

(iii) Since $|X| = \phi(a)$, $|Y| = \phi(b)$, then $\phi(ab) = |Z| = |X \times Y| = \phi(a)\phi(b)$ by the bijection established in the previous part.

(d) Applying part (c) inductively, we conclude that

$$
\begin{aligned}
\phi(n) &= \phi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) \\
&= \prod_{i=1}^{k} \phi(p_i^{e_i}) \\
&= \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1} \\
&= \prod_{i=1}^{k} \frac{p_i - 1}{p_i} p_i^{e_i} \\
&= n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}.
\end{aligned}
$$

3 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 $S = \{m_1, m_2, \ldots, m_{\phi(n)}\}$. Show that the set

$$S' = \{am_1 \pmod{n}, am_2 \pmod{n}, \ldots, am_{\phi(n)} \pmod{n}\}$$

is a permutation of S. (Hint: Recall the FLT proof.)

(b) Prove Euler's Totient Theorem. (Hint: Continue to recall the FLT proof.)

(c) Note 7 gave two proofs for Theorem 7.1:

$$x^{ed} \equiv x \pmod{N}$$

Use Euler's Totient Theorem to give a third proof of this theorem, for the case that $\gcd(x,N) = 1$.

Solution:

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

First, we show that if 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.

Now, we show that each $a \cdot m_i$ are distinct from each other. Assuming for the sake of contradiction that $a \cdot m_i \equiv a \cdot m_j \pmod{n}$, we can multiply both sides by the multiplicative inverse of a to get $m_i \equiv m_j \pmod{n}$, contradiction.

Therefore, S' has $\phi(n)$ elements, each of which is a distinct element of S, thus S' must contain each element of S exactly once. Therefore, S is a permutation of S.

Alternate Solution I: We can also prove this using set theory. Showing that each $a \cdot m_i \pmod{n}$ is coprime to n tells us that each element of S' is contained in S, thus $S' \subseteq S$. Additionally, consider an arbitrary element m_i in S. We know that $a^{-1} \cdot m_i \pmod{n}$ is a number coprime to n, so it must be in S. Then, $a \cdot (a^{-1} \cdot m_i) \pmod{n} = m_i$ is in S', so $S \subseteq S'$. Thus, $S = S'$.

Alternate Solution II: We can also prove this by showing that

$$f : \{m_1, m_2, \ldots, m_{\phi(n)}\} \to \{m_1, m_2, \ldots, m_{\phi(n)}\}$$

is a bijection, where $f(x) := ax \pmod{n}$. We first note that since m_i and a are both coprime to n, so is $a \cdot m_i$. 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,

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

Since $m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)}$ is relatively prime to n, we can multiply both sides by its inverse to get

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

(c) Since $N = pq$ for primes p, q, we know that

$$\phi(N) = \phi(p)\phi(q) = (p-1)(q-1)$$

Thus, we can express x^{ed} as follows:

$$x^{ed} = x^{k\phi(N)+1} = x \cdot x^{k\phi(N)}$$

By Euler's theorem, since $x^{\phi(N)} \equiv 1 \pmod{N}$, we have

$$x^{ed} \equiv x \cdot 1 \equiv x \pmod{N}$$

4 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 $n+1, n+2, n+3, \dots, n+k$ 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, $p_1, p_2, \dots, p_{2k}$, 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!

5 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) Encrypt your answer from part (b) to check its correctness.

Solution:

(a) The private key d is defined as the inverse of $e \pmod{(p-1)(q-1)}$. Thus we need to compute $9^{-1} \bmod (5-1)(11-1) = 9^{-1} \bmod 40$. Compute $\text{egcd}(40, 9)$:

$$\begin{aligned}
\text{egcd}(40,9) &= \text{egcd}(9,4) && [4 = 40 \bmod 9 = 40 - 4(9)] \\
&= \text{egcd}(4,1) && [1 = 9 \bmod 4 = 9 - 2(4)]. \\
1 &= 9 - 2(4). \\
1 &= 9 - 2(40 - 4(9)) \\
&= 9 - 2(40) + 8(9) = 9(9) - 2(40).
\end{aligned}$$

We get $-2(40) + 9(9) = 1$. So the inverse of 9 is 9. So $d = 9$.

(b) 4 is the encrypted message. We can decrypt this with $D(m) \equiv m^d \equiv 4^9 \equiv 14 \pmod{55}$. Thus the original message was 14.

(c) The answer from the second part was 14. To encrypt the number x we must compute x^e mod N. Thus, $14^9 \equiv 14 \cdot (14^2)^4 \equiv 14 \cdot (31^2)^2 \equiv 14 \cdot (26^2) \equiv 14 \cdot 16 \equiv 4 \pmod{55}$. This verifies the second part since the encrypted message was supposed to be 4.

6 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 $e, d > 1$ 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 $D(E(x)) = x$.

Solution:

(a) Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.
We want to show x is recovered by $E(x)$ and $D(y)$, such that $D(E(x)) = x$.
In other words, $x^{ed} \equiv x \pmod{p}$ for all $x \in \{0, 1, \ldots, N-1\}$.
Proof: By construction of d, we know that $ed \equiv 1 \pmod{p-1}$. This means we can write $ed = k(p-1)+1$, for some integer k, and $x^{ed} = x^{k(p-1)+1}$.

- x is a multiple of p: Then this means $x = 0$, and indeed, $x^{ed} \equiv 0 \pmod{p}$.
- x is not a multiple of p: Then

$$
\begin{aligned}
x^{ed} &\equiv x^{k(p-1)+1} \pmod{p} \\
&\equiv x^{k(p-1)} x \pmod{p} \\
&\equiv 1^k x \pmod{p} \\
&\equiv x \pmod{p},
\end{aligned}
$$

by using FLT.

And for both cases, we have shown that x is recovered by $D(E(x))$.

(b) Since Eve knows $N = p$, and $d \equiv e^{-1} \pmod{p-1}$, now she can compute d using EGCD.

(c) Let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N, e) and calculate $d = e^{-1} \pmod{(p-1)(q-1)(r-1)}$. People who wish to send me a secret, x, send $y = x^e \pmod{N}$. We decrypt an incoming message, y, by calculating $y^d \pmod{N}$.

Does this work? We prove that $x^{ed} - x \equiv 0 \pmod{N}$, and thus $x^{ed} = x \pmod{N}$.
To prove that $x^{ed} - x \equiv 0 \pmod{N}$, we factor out the x to get
$x \cdot (x^{ed-1} - 1) = x \cdot (x^{k(p-1)(q-1)(r-1)+1-1} - 1)$ because $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$.

We now show that $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$ is divisible by p, q, and r. Thus, it is divisible by N, and $x^{ed} - x \equiv 0 \pmod{N}$.
To prove that it is divisible by p:

- if x is divisible by p, then the entire thing is divisible by p.
- if x is not divisible by p, then that means we can use FLT on the inside to show that $(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{p}$. Thus it is divisible by p.

To prove that it is divisible by q:

- if x is divisible by q, then the entire thing is divisible by q.
- if x is not divisible by q, then that means we can use FLT on the inside to show that $(x^{q-1})^{k(p-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{q}$. Thus it is divisible by q.

To prove that it is divisible by r:

- if x is divisible by r, then the entire thing is divisible by r.
- if x is not divisible by r, then that means we can use FLT on the inside to show that $(x^{r-1})^{k(p-1)(q-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{r}$. Thus it is divisible by r.