CS 70 Fall 2020 Discrete Mathematics and Probability Theory HW 4

1 Fibonacci GCD

The Fibonacci sequence is given by $F_n = F_{n-1} + F_{n-2}$, where $F_0 = 0$ and $F_1 = 1$. Prove that, for all $n \geq 0$, $\gcd(F_n, F_{n-1}) = 1$.

Solution:

Proceed by induction.

Base Case: We have $\gcd(F_1, F_0) = \gcd(1, 0) = 1$, which is true.

Inductive Hypothesis: Assume we have $\gcd(F_k, F_{k-1}) = 1$ for some $k \geq 1$.

Inductive Step: Now we need to show that $\gcd(F_{k+1}, F_k) = 1$ as well.

We can show that:

$$\gcd(F_{k+1}, F_k) = \gcd(F_k + F_{k-1}, F_k) = \gcd(F_k, F_{k-1}) = 1.$$

Note that the second expression comes from the definition of Fibonacci numbers. The last expression comes from Euclid's GCD algorithm, in which $\gcd(x, y) = \gcd(y, x \bmod y)$, since

$$F_k + F_{k-1} \equiv F_{k-1} \pmod{F_k}.$$

Therefore the statement is also true for $n = k + 1$.

By the rule of induction, we can conclude that $\gcd(F_n, F_{n-1}) = 1$ for all $n \geq 1$, where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.

2 The Last Digit

In each case show your work and justify your answers.

(a) If $9k + 5$ and $2k + 1$ have the same last digit for some natural number k, find the last digit of k.

(b) If $S = \sum_{i=1}^{19} i!$, then find the last digit of S^2.

Solution:

(a) We have

$$\begin{aligned} 9k + 5 &\equiv 2k + 1 \pmod{10}, \\ 7k &\equiv -4 \pmod{10}, \\ 7k &\equiv 6 \pmod{10}. \end{aligned}$$

Now since gcd(7,10)=1, 7 has a (unique) inverse mod 10, and since $7 \times 3 = 21 \equiv 1 \pmod{10}$ the inverse is 3. We multiply both sides of $7k \equiv 6 \pmod{10}$ by 3:

$$k \equiv 18 \equiv 8 \pmod{10}.$$

Hence, the last digit of k is 8.

(b) Note that for $n \geq 5$:

$$n! = \left(\prod_{i=6}^{n} i\right) \times 5! = \left(\prod_{i=6}^{n} i\right) \times 120 \equiv 0 \pmod{10}.$$

So we have:

$$S = \sum_{i=1}^{19} i! = 1! + 2! + 3! + 4! + \sum_{i=5}^{19} i! = 1 + 2 + 6 + 24 + 0 \equiv 3 + 0 \pmod{10}.$$

Then, for S^2:

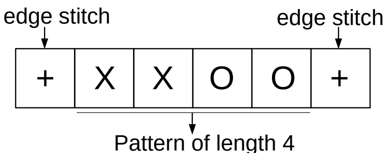
$$S^2 \equiv 9 \pmod{10}.$$

Hence, the last digit of S^2 is 9.

3 Celebrate and Remember Textiles

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).

+	X	X	O	O	X	X	O	O	X	X	O	O	+

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

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

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

and

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

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.

4 Sparsity of Primes

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

Solution:

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

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

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

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

5 Fermat's Little Theorem

Fermat's Little Theorem states that for any prime p and any $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$. Without using induction, prove that $\forall n \in \mathbb{N}$, $n^7 - n$ is divisible by 42.

Solution:

Let $n \in \mathbb{N}$. We begin by breaking down 42 into prime factors: $42 = 7 \times 3 \times 2$. Since 7, 3, and 2 are prime, we can apply Fermat's Little Theorem, which says that $a^p \equiv a \pmod{p}$, to get the congruences

$$\begin{aligned}
n^7 &\equiv n \pmod{7}, && (1) \\
n^3 &\equiv n \pmod{3}, \qquad \text{and} && (2) \\
n^2 &\equiv n \pmod{2}. && (3)
\end{aligned}$$

Now, let's take (2) and multiply it by $n^3 \cdot n$. This gives us

$$n^7 \equiv n^3 \cdot n^3 \cdot n \equiv n \cdot n \cdot n \equiv n^3 \pmod{3},$$

and since by (2), $n^3 \equiv n \pmod{3}$, this gives

$$n^7 \equiv n \pmod{3}.$$

Similarly, we take (3) and multiply by $n^2 \cdot n^2 \cdot n$ to get

$$n^7 \equiv n^2 \cdot n^2 \cdot n^2 \cdot n \equiv n^4 \pmod{2}.$$

Notice that $n^4 \equiv n^2 \cdot n^2 \equiv n \cdot n \equiv n^2 \pmod{2}$, and by (3) $n^2 \equiv n \pmod{2}$, so we have

$$n^7 \equiv n \pmod{2}.$$

Thus,

$$\begin{aligned} n^7 &\equiv n \pmod{7}, && (4)\\ n^7 &\equiv n \pmod{3}, \qquad \text{and} && (5)\\ n^7 &\equiv n \pmod{2}. && (6) \end{aligned}$$

Let $x = n^7 - n$. By the Chinese Remainder Theorem, the system of congruences

$$\begin{aligned} x &\equiv 0 \pmod{7}\\ x &\equiv 0 \pmod{3}\\ x &\equiv 0 \pmod{2} \end{aligned}$$

has a unique solution modulo $2 \cdot 3 \cdot 7 = 42$, and this unique solution is $x \equiv 0 \pmod{42}$. So, we have that $n^7 - n \equiv 0 \pmod{42}$, which means $n^7 - n$ is divisible by 42.

6 A Taste of RSA

Suppose that p and q are distinct odd primes (i.e. they are primes > 2). Define $N = pq$. Let a be any integer that is relatively prime to N. In other words, $\gcd(a,N) = 1$. Prove that $a^{(p-1)(q-1)+1} \equiv a \pmod{N}$. It turns out that this equivalence is in fact the basis of RSA, as you will see soon in class.

Solution:

Note: This problem is essentially asking you to prove the correctness of RSA.

We know that a is not a divsible by p and a is not divisible by q since $\gcd(a, pq) = 1$.We subtract a from both sides to get

$$\begin{aligned} a^{(p-1)(q-1)+1} - a &\equiv 0 \pmod{pq}\\ a(a^{(p-1)(q-1)} - 1) &\equiv 0 \pmod{pq} \end{aligned}$$

Since p,q are primes, we just need to show that the left hand side is divisible by both p and q. Since a is not divisible by p, we can use Fermat's Little Theorem to state that $a^{p-1} \equiv 1 \pmod{p}$.

$$a\big((a^{(p-1)})^{q-1} - 1\big) \equiv a(1^{q-1} - 1) \equiv 0 \pmod{p}$$

Thus $a(a^{(p-1)(q-1)} - 1)$ is divisible by p. We can apply the same reasoning to show that the expression is divisible by q. Therefore we have proved our claim that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

Alternative Proof:
Because $\gcd(a, pq) = 1$, we have that a does not divide p and a does not divide q. By Fermat's Little Theorem,

$$a^{(p-1)(q-1)+1} = (a^{(p-1)})^{(q-1)} \cdot a \equiv 1^{q-1} \cdot a \equiv a \pmod{p}.$$

Similarly, by Fermat's Little Theorem, we have

$$a^{(p-1)(q-1)+1} = (a^{(q-1)})^{(p-1)} \cdot a \equiv 1^{p-1} \cdot a \equiv a \pmod{q}.$$

Now, we want to use this information to conclude that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$. We will first take a detour and show a more general result (you could write this out separately as a lemma if you want).

Consider the system of congruences

$$\begin{aligned} x &\equiv a \pmod{p} \\ x &\equiv a \pmod{q}. \end{aligned}$$

Let's run the CRT symbolically. First off, since p and q are relatively prime, we know there exist integers g, h such that

$$g \cdot p + h \cdot q = 1.$$

We could find these via Euclid's algorithm. By the CRT, the solution to our system of congruences will be

$$x \equiv a \cdot y_1 \cdot q + a \cdot y_2 \cdot p \pmod{pq}.$$

To solve for y_1 and y_2, we must find y_1 such that

$$x_1 \cdot p + y_1 \cdot q = 1$$

and y_2 such that

$$x_2 \cdot q + y_2 \cdot p = 1.$$

This is easy since we already know $g \cdot p + h \cdot q = 1$: the answers are $y_1 = h$ and $y_2 = g$. Finally we can plug in to the solution to get

$$x \equiv a \cdot h \cdot q + a \cdot g \cdot p \equiv a(h \cdot q + g \cdot p) \equiv a \cdot 1 \equiv a \pmod{pq}.$$

Therefore by the CRT we know that the set of solutions that satisfy both $x \equiv a \pmod{p}$ and $x \equiv a \pmod{q}$ is exactly the set of solutions that satisfy $x \equiv a \pmod{pq}$.

So since $a^{(p-1)(q-1)+1} \equiv a \pmod{p}$ and $a^{(p-1)(q-1)+1} \equiv a \pmod{q}$, then by the CRT we know that $a^{(p-1)(q-1)+1}$ satisfies $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.