CS 70   Discrete Mathematics and Probability Theory

Fall 2020   HW 4

Due: Friday 09/25 at 10:00 PM

Grace period until Friday 09/25 at 11:59 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 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 $n \geq 0$, $\gcd(F_n, F_{n-1}) = 1$.

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.

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.

edge stitch   edge stitch

| + | X | X | O | O | + |
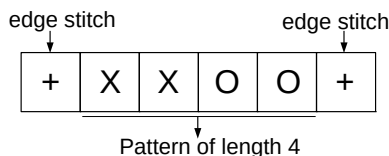
Pattern of length 4

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.**

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

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 $a^{p-1} \equiv 1$ (mod p). Without using induction, prove that $\forall n \in \mathbb{N}$, $n^7 - n$ 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 $a^{(p-1)(q-1)+1} \equiv a$ (mod N). It turns out that this equivalence is in fact the basis of RSA, as you will see soon in class.