Problem Set 3a

Released: August 24, 2021

1. How many zeros does the integer 100! end with (when written in decimal)?

2. Prove or disprove that $n^2 - 79n + 1601$ is prime whenever n is a positive integer.

3. Prove or disprove that for every two positive integers a, b, if an integer linear combination of a and b^2 equals 1, then so does an integer linear combination of a^2 and b.

4. Show that if $2^m + 1$ is an odd prime, then $m = 2^n$ for some non negative integer n.

   Hint: If m is not a power of 2, then it has an odd factor $k > 1$. Can you factorize $2^{tk} + 1$? You can use the fact that for any integers a, b and positive integer k, it holds that $(a - b)|(a^k - b^k)$. You could prove this fact using strong induction by noting that $a^{k+1} - b^{k+1} = (a^k - b^k)(a + b) - (a^{k-1} - b^{k-1})ab$.

5. Recall the *Skippy Clock* from the lecture: It has numbers $0, 1, .., m - 1$ on its dial, and the needle, starting at 0, moves a steps at a time (i.e., hits numbers $0, a, 2a, \dots$). Show that needle will hit exactly all the multiples of $\gcd(a, m)$ that are on the dial.

   Hint: You can use the fact that the "one-dimensional lattice" $L(a, m) \triangleq \{au + mv | u, v \in \mathbb{Z}\}$ consists of exactly all the multiples of $\gcd(a, m)$. However, note that in defining $L(a, m)$, u and v can be negative, whereas the clock's needle moves only clockwise.

6. Here is a game you can analyze with what you have learnt in class and always beat me. We start with two positive integers, a, b, written on a blackboard such that $a > b$ and $\gcd(a, b) = 1$. Now we take turns. I'll let you decide who goes first after seeing a, b. At each turn, the player must write a *new* positive integer on the board that is the difference of two numbers that are already there. If a player cannot play, then they lose.

   For example, suppose $a = 5$, $b = 3$ and you choose to make the first move. Then your first move must be to play $5 - 3 = 2$. Then I can play $1 = 3 - 2$ (I cannot play $5 - 2 = 3$ as it is already on the board). You can play $5 - 1 = 4$. At this point I cannot make a move, and I lose.

   (a) Show that the game must terminate, and when it terminates, every integer in the range $[1, a]$ is on the board.

   (b) Describe a strategy that lets you win this game every time.

7. A number is said to be *perfect* if it is equal to the sum of its positive divisors, other than itself. The smallest perfect number is 6 (with $6 = 1 + 2 + 3$, where 1, 2, 3 are its divisors, excluding itself). Around 300 B.C., Euclid proved that *if* $2^n - 1$ is a prime number[1] then $(2^n - 1)2^{n-1}$ is a perfect number. Can you prove this result of Euclid?

8. Find all $m \in \mathbb{Z}^+$ such that, for all integers a, b, $a^2 \equiv b^2 \pmod{m}$ iff $a \equiv b \pmod{m}$.

9. Suppose $m \in \mathbb{Z}^+$. Show that every $a \in \mathbb{Z}_m$ has at most one multiplicative inverse in $\mathbb{Z}_m$.

10. Suppose $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$. Show that there is an integer x such that $ax \equiv b \pmod{m}$ iff $\gcd(a, m)|b$. Describe an algorithm to find a solution when it exists. (You can use the algorithms covered in the lectures.)

[1] Such a prime number is called a Mersenne prime. To date, only 51 such numbers are known, the largest of which was discovered in December 2018. The last 17 such discoveries were made by *The Great Internet Mersenne Prime Search* (GIMPS), a project that started in 1996.