Number Theory and the Euclidean Algorithm

JV Practice 2/14/21

Zoe Wellner

1 Background and Review

Recall from last time, we consider a and b congruent modulo n, written as $a \equiv b \mod n$ when b is the reminder of a divided by n. In other words, n divides $a - b$. Modulo has the following basic properties given $a \equiv b \mod n$ and $c \equiv d(\mod n)$:

- $a + c \equiv b + d \pmod n$
- $a - c \equiv b - d \pmod n$
- $a \cdot c \equiv b \cdot d \pmod n$

Recall that we don't always have a multiplicative inverse (the ability to divide). For a, a^{-1} will be such that $aa^{-1} = 1 \pmod n$. We also saw that a^{-1} exists if and only if a and n are coprime, so $\gcd(a, n) = 1$

2 Warmup

1. (Challenge problem from last time that we will cover at the beginning of today.) Show that $(p-1)! \equiv -1 \pmod p$ whenever p is prime
2. Find the greatest common divisor of 102 and 38, i.e. calculate $\gcd(102, 38)$
3. Find the integers x, y such that $102x + 38y = \gcd(102, 38)$
4. Find the greatest common divisor for $n! + 1$ $(n + 1)! + 1$ in terms of n

3 Problems

1. Find the greatest common divisor of 7544 and 115, i.e. calculate $\gcd(7544, 115)$
2. Find the integers x, y such that $7544x + 115y = \gcd(7544, 115)$
3. Prove that $27x + 4$ and $18x + 3$ are coprime for any integer x
4. The least common multiple of a and b is 12 and the least common multiple of b and c is 15. What is the smallest possible value for the least common multiple of a and c?
5. What is the ratios of the least common multiple of 180 and 594 to the greatest common factor of 180 and 594?

6. Let S be the set of all positive integers less than 1000, such that when written in binary has, at most two 1s. If a number is chosen from S uniformly at random, what is the probability that it is divisible by 9?

7. Consider the sequence $x, x^2, x^3, \dots \pmod{13}$, this is always periodic. What are all possible periods (length at which it repeats) for this sequence?