Number theory problems

Cyril and Zac

February 2023

1 Problems

1. What is $57 \times 19 \bmod 13$.
Solution: $57 \times 19 \equiv 5 \times 6 = 30 \equiv 4 \bmod 13$

2. Evaluate $\gcd(52, 91)$.
Solution: $\gcd(52, 91) = \gcd(52, 91 - 52) = \gcd(52, 39) = \gcd(52 - 39, 39) = \gcd(13, 39) = \gcd(13, 39 - 13 \times 2) = \gcd(13, 13) = 13$

3. Evaluate $5^{123} \bmod 7$.
Solution: $5^{123} = 5^{120} \times 5^3 = \left(5^{20}\right)^6 \times 5^3 \equiv 1 \times (-2)^3 = -8 \equiv 6 \bmod 7$

4. Prove that for all integers n with $n \geq 3$, if $2^n - 1$ is prime, then n cannot be even.
Solution: If n is even, then $n = 2k$ for some integer k. So,

$$2^n - 1 = \left(2^k\right)^2 - 1 \equiv 1 - 1 = 0 \bmod 3$$

. This means $2^n - 1$ is divisible by 3, so $2^n - 1$ being prime must imply n is not even (otherwise $2^n - 1$ would not be prime, which would result in a contradiction)

5. (Wilson's theorem) Show that $(p-1)! = -1 \pmod{p}$ for prime p.

Hint: Consider inverses
Solution: Consider $x^2 \equiv 1 \bmod p$. This can be simplified to $(x-1)(x+1) \equiv 0 \bmod p$. Since p is prime, $(x-1)$ is entirely divisible by p or $(x+1)$ is entirely divisible by p (no other way to split up the factors of p). So, $x \equiv 1$ or $x \equiv -1$.

Since every integer $0 < x < p$ is coprime to p, it has a unique inverse, which means inverses exist in distinct pairs except for 1 and $p - 1$. Thus, if p is an odd prime, $(p-1)! \equiv 1 \times 1^{\frac{p-3}{2}} \times (p-1) = (p-1) \equiv -1 \bmod p$. If $p = 2$, then $(p-1)! = 1! = 1 \equiv -1 \bmod 2$.

6. Prove that among any three distinct integers we can find two, say a and b, such that the number $a^3b - ab^3$ is a multiple of 10.

Solution: We may rewrite this as $ab(a^2 - b^2) = ab(a-b)(a+b)$. If a and b are odd, then $(a-b) \equiv 0 \bmod 2$, so $ab(a-b)(a+b) \equiv 0 \bmod 2$. If either of a or b are even, then $ab(a-b)(a+b) \equiv 0 \bmod 2$. Thus in both cases the same result holds.

Now, suppose there exist three integers such that we can choose two, a and b, where $ab(a-b)(a+b) \not\equiv 0 \bmod 5$. Then we require $a \not\equiv 0 \bmod 5$, $b \not\equiv 0 \bmod 5$ and $a \not\equiv b \bmod 5$. So, the three integers must be distinct and, under mod 5, must take on three values from $\{1, 2, 3, 4\}$. However, we can always choose two values such that $a + b \equiv 0 \bmod 5$; if 2 or 3 is not one of our choices, then we choose $a \equiv 1 \bmod 5$ and $b \equiv 4 \bmod 5$, and if 1 or 4 is not selected, then we choose $a \equiv 2 \bmod 5$ and $b \equiv 3 \bmod 5$. Thus, by contradiction, $ab(a-b)(a+b) \equiv 0 \bmod 5$.

Since, we can choose two values a and b from three integers such that

$$ab(a-b)(a+b) \equiv 0 \bmod 5,$$

and these integers also have the property that

$$ab(a-b)(a+b) \equiv 0 \bmod 2,$$

it must be that $ab(a-b)(a+b) \equiv 0 \bmod 10$.

7. Define the function $f(x, y)$ for positive integers x, y as:

$$f(x,y) = \left\{ \begin{array}{ll} f(y, x \bmod y) + 1 & \text{for } x, y > 1 \\ 0 & \text{else} \end{array} \right\}$$

where $x \bmod y$ refers to the remainder after calculating $x \div y$. Find two values $x \leq y \leq 90$ for which $f(x, y)$ attains its maximum.

Solution: This function essentially simulates the Euclidean algorithm and "returns" the number of steps. Consider the process in reverse: we would start off with two integers $a \leq b$ and add a multiple of the smaller to the larger. To maximise the number of steps, we want to add the smallest possible multiple to the other number (i.e. itself). We can express this as a recurrence relation:

$$F_1 = a, F_2 = b, F_n = F_{n-1} + F_{n-2}$$

. Hm... where have I seen this? Starting with $1, 2$ results in $55, 89$ in 8 steps, and no other valid a, b results in both values being less than or equal to 90 in 8 steps (one of a, b must be greater than 1 otherwise $f(a, b)$ is unattainable). So $f(55, 89)$ achieves the maximum for $x, y \leq 90$.

8. Define the sequence of integers $a_1, a_2, a_3, ...$ by $a_1 = 1$, and

$$a_{n+1} = (n + 1 - \gcd(a_n, n))a_n$$

for all integers $n \geq 1$. Prove that $\frac{a_{n+1}}{a_n} = n$ if and only if n is prime or $n = 1$. (Simon Marais 2021)
Solution: Let's use strong induction (yadda yadda base case whatever).
Assume statement is true for all positive integers $n \leq k-1$, where $k-1$ is a positive integer.
If $k = 1$, then $\frac{a_{k+1}}{a_k} = k + 1 - \gcd(a_k, 1) = k + 1 - 1 = k$.

If k is prime, then for all $n < k$, since $\frac{a_{n+1}}{a_n} = n + 1 - \gcd(a_n, n) \leq n$ (as $\gcd(a_n, n) \geq 1$), $k \nmid \frac{a_{n+1}}{a_n}$. Moreover, since k is prime, $\gcd(k, \frac{a_{n+1}}{a_n}) = 1$. So, we evaluate:

$$\gcd(k, a_k) = \gcd\left(k, \frac{a_k}{a_{k-1}} \times \frac{a_{k-1}}{a_{k-2}} \times \cdots \times \frac{a_2}{a_1} \times 1\right) = 1.$$

Therefore $\frac{a_{k+1}}{a_k} = k + 1 - 1 = k$.

If k is composite, then it is divisible by some prime p where $p < k$. From our induction hypothesis, we know $\frac{a_{p+1}}{a_p} = p$. So, because $\frac{a_{p+1}}{a_p} | a_k$, $\gcd(a_k, k) \geq p > 1$, thus $\frac{a_{k+1}}{a_k} = k + 1 - \gcd(a_k, k) < k$.