Divisibility and Congruences (I)

Jongmin Lim (March 2022)

February 23, 2022

1 Things you should be able to do at the end of this lecture

1. Bezout Identity, Fermat's little theorem, Euler's theorem, Wilson's Theorem
2. McNugget Theorem
3. Insane factorisations

2 Warm-up

1. Show that if $p, p+11, p^2+4$ are all primes, then p^6+p^3+5 is also a prime.
2. Find all $x, y \in \mathbb{Z}^+$ such that $\frac{1}{x}+\frac{1}{y}=\frac{1}{2022}$
3. Find all $n \in \mathbb{Z}^+$ such that $n+10|n^3+100$.
4. Find all $n \in \mathbb{Z}^+$ such that $\frac{1}{3}+\frac{1}{n}$ can be expressed as a fraction with a denominator less than n.
5. Show that $\frac{12n+1}{30n+2}$ is irreducible for all $n \in \mathbb{Z}^+$.
6. Notice that in base 10, we have $12 = 3 \times 4$ and $56 = 7 \times 8$. Notice that we have four consecutive digits. Find another such equation, perhaps in another base system, such that the digits are in an arithmetic sequence with difference two.
7. Let $x, y \in \mathbb{Z}^+$ such that $lcm(x, y) + gcd(x, y) = x + y$. Show that one of the numbers is divisible by the other.

3 Fun facts

1. If $x, y \in \mathbb{Z}$ and $xy = n$, then x, y are divisors of n.
2. If $x, y \in \mathbb{Z} \setminus \{0\}$, then there exist $q, r \in \mathbb{Z}$ such that $0 \le r \le y-1$ such that $x = yq + r$.
3. $\gcd(x, y) = \gcd(y, r)$.
4. Let $gcd(a, b) = 1$. Then there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. (Bezout's Identity)
5. If x_0, y_0 are such that $ax_0 + by_0 = 1$, then
$$\{(x, y) \in \mathbb{Z} \mid ax + by = 1\} = \{(x_0 - ky, y_0 + kx) \mid k \in \mathbb{Z}\}$$
6. Let p be prime. Then $\{1, 2, \cdots, p-1\} \equiv \{a, 2a, \cdots (p-1)a\} \pmod{p}$ for all $a \in \mathbb{Z}$ such that $p \not| a$.
7. Thus $a^{p-1} \equiv 1 \pmod{p}$.
8. Actually, let p be any number. Let $R = \{n \in \mathbb{Z} \mid 0 < n < p,\ gcd(n, p) = 1\}$. Then for any $gcd(a, n) = 1$, let $aR = \{an \mid n \in R\}$. Then $aR \equiv R \pmod{p}$.
9. Thus, $a^{|R|} \equiv 1 \pmod{p}$. Let $\phi : \mathbb{N} \to \mathbb{N}$ such that $\phi(p) = |R|$. This is the Euler totient function.
10. Wait, there's more! Let p be prime again. Then $(p-1)! \equiv -1 \pmod{p}$. This is Wilson's Theorem.

4 McNugget Theorem

Unfortunately, Mcdonalds sells chicken nuggets in packs of a and b, where a, b are coprime positive integers. What is the greatest integer N such that we cannot order N chicken nuggets with these packs?

1. Let's do some experiments. Everybody split up and do some small cases.
2. Let's have a guess on what N can be in terms of a and b.
3. A number M is order-able when we can find positive integers x, y such that $ax + by = M$. Let's try to prove that $N + 1$ is order-able. (fun fact number 5 wink wink)
4. Can you prove that every order greater than N is order-able?
5. Find a pattern that tells you how many numbers $0 \leq n \leq N - 1$ are order-able.

5 Insane factorisations

To use fun fact number 1, we need to have great powers in factorising. Please flex your factorisation muscles.

1. Find all $n \in \mathbb{Z}$ such that $n^2 + 3n + 1$ divides $n^3 + 6n^2 + 2n + 1$.
2. Factorise fully with rational coefficients.
   (a) $x^2 - y^2 + 2y - 1$
   (b) $x^2 - y^2 - 4x + 2y + 3$
   (c) $x^4 + x^2 + 1$
   (d) $x^4 + 4$
   (e) $x^5 + x^4 + 1$
   (f) $(a + b + c)(ab + bc + ca) - abc$ (Ok, this one isn't really number theory but it's cool nonetheless)
3. Find $\sqrt{1000 \times 1001 \times 1002 \times 1003 + 1}$
4. Let $P(x) = x^2 + x + 1$ for positive integers x. Let $Q(x)$ be the smallest prime divisor of $P(x)$. Show that $Q(x)$ is never eventually monotonically increasing.
5. (Hard) Show that if $4^n + 2^n + 1$ is prime, then n must be a power of 3.

6 Cyclic numbers

It was a warm mid summer's day in 2013, where a Year 9 Jongmin was studiously preparing for the upcoming mathematics competitions. As he was chugging along the questions, he ran into a quite an interesting problem. The problem read,

Find all numbers n such that when we multiply n by 5, the ones digit of n becomes the leading digit, and every other digit shifts down by one. For example, 147 → 714

1. Let's discuss ideas to solve this question.
2. What if the number has this property when multiplied by 2 instead? Or 3? Or any other number?

7 Problems

1. Show that for every prime p, there exists a number of the form $9999 \cdots 999$ which is divisible by p
2. Hence or otherwise, show that $\frac{1}{p}$ is expressable as a recurring decimal number.
3. Hence or otherwise, show that every rational number is expressable as a recurring decimal number.
4. Let positive integers a, b, c satisfy $c(ac + 1)^2 = (5c + 2b)(2c + b)$. If c is odd, show that it must be a perfect square.
5. Find all triples of positive integers a, b, c such that $\frac{(at+1)(bt+1)(ct+1)-1}{lcm(at,bt,ct)}$ is an integer.
6. Prove that $\left\lfloor \frac{(n-1)!}{n(n+1)} \right\rfloor$ is even for every $n \in \mathbb{Z}^+$