workshop 5 solutions

Cyril Subramanian and Haibing Wang

April 2023

1 Introduction

1. Show that $7|x^2 + y^2$ iff $7|x$ and $7|y$ (use quadratic residues).
   Solution: The quadratic residues under mod 7 are $0, 1, 2, 4$. The only pair whose members are from this set and add to 0 are $0, 0$, thus x and y are $0 \pmod 7$. The other direction is trivial

2. If $7|a^3 + b^3 + c^3$, how many of a, b, c could be divisible by 7? (use cubic residues).
   Solution: The cubic residues of 7 are $-1, 0, 1$. The only ways to make three of theses add to 7 are $\{0, 0, 1\}$ or $\{-1, -1, 1\}$.

3. Do there exist three squares summing to 7007?
   Solution: Under mod 8, the quadratic residues are $0, 1, 4$. $7007 \equiv 7 \pmod 8$, and no three of these quadratic residues add to $7 \pmod 8$.

4. Prove there are no integer solutions to
   $$x^2 - 2y^2 = 10.$$
   Solution: Under mod 5, the quadratic residues are $0, 1, 4$. $10 + 2y^2$ can thus only take up the values $10 + 2 \cdot 0^2 \equiv 0, 10 + 2 \cdot 1^2 \equiv 2, 10 + 2 \cdot 4^2 \equiv 2$. Evidently, the only of these which are quadratic residues are when x, y are multiples of 5, so $x^2 - 2y^2$ is a multiple of 25 (the LHS), while the RHS is not.

5. Find all integer solutions to $a^3 + 2b^3 = 7a^2b$.
   Solution: The only way for $a^3 + 2b^3$ to be $7a^2b \equiv 0 \pmod 7$ (because of cubic residues) is if $a \equiv b \equiv 0 \pmod 7$. Note this means $\frac{a}{7}$ and $\frac{b}{7}$ are integers and, upon substitution, clearly satisfy the equation. Thus, infinite descent shows there are no non-zero solutions as non-zero integers can only be divided by 7 a finite number of times before they are no longer integers. Thus, $a = b = 0$ is the only set of integer solutions.

6. Prove there are infinite primes 3 mod 4.
   Solution: Suppose there are finite number of 3 mod 4 primes, denoting them as $p_1, \ldots, p_n$. Then, if their product $p_1 \ldots p_n$ is:

- $1 \; mod \; 4$, $p_1 p_2 \dots p_n + 2 \equiv 0 + 2 = 2 \not\equiv 0 \pmod{p_i}$, for all $1 \le i \le n$
- $3 \; mod \; 4$, $p_1 p_2 \dots p_n + 4 \equiv 0 + 4 = 4 \not\equiv 0 \pmod{p_i}$, for all $1 \le i \le n$ (note $p_i \neq 2$).

Each constructed number must be divisible by at least one 3 mod 4 prime, since if not then the resulting number would be 1 mod 4. Therefore, by contradiction, there must be infinite 3 mod 4 primes.

7. Given p, q are coprime, find the value of

$$\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \dots + \left\lfloor \frac{(q-1)p}{q} \right\rfloor.$$

Solution: The fractional part of each $\frac{kp}{q}$ for $k = 0$ to $q-1$ takes on a different value under mod q divided by q (since multiples of a coprime number under a modulus permute through all possible numbers in that modulus), thus the resulting sum equals

$$\sum_{k=1}^{q-1} \frac{kp}{q} - \sum_{k=1}^{q-1} \frac{k}{q} = \frac{pq(q-1)}{2q} - \frac{q(q-1)}{2q} = \frac{(p-1)(q-1)}{2}$$

8. (Gauss' Lemma) An odd prime p is congruent to 1 mod 4 iff there exists x such that $x^2 \equiv -1$ mod p.
Solution: If $x^2 \equiv -1 \pmod{p}$, $x \not\equiv 1 \pmod{p}$, so $x^3 \not\equiv 1 \pmod{p}$, but $x^4 \equiv 1 \pmod{p}$. Thus 4 is the smallest positive k where $x^k \equiv 1 \pmod{p}$, so $4|p-1$ (see first property from workshop slides)
Note that

$$1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} \cdot \left(\frac{p-1}{2} + 1\right) \cdot \dots \cdot (p-1) = \left(\frac{p-1}{2}\right)! \cdot (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! = -1,$$

by Wilson's theorem. Thus, if $p - 1 \equiv 0 \pmod{4}$, then $\frac{p-1}{2}$ is even, so $\left(\frac{p-1}{2}\right)!^2 = -1$.

9. Find all consecutive integer powers of 2 and 3 (in either order).
Solution: Consider two cases:

   - $2^n - 1 = 3^m$ for integers n, m. If n is odd, $2^n - 1 \equiv (-1)^n - 1 = -1 - 1 \equiv 1 \pmod{3}$. The only power of 3 which is 1 mod 3 is $1 = 2^1 - 1$, and no other odd n make this work. If n is even, note that $2^n - 1$ can be a power of 3 only if $2^{\frac{n}{2}} - 1$ is a power of 3 (but this is not a guarantee) since $\frac{n}{2}$ is an integer, and $2^n - 1 = (2^{\frac{n}{2}} - 1)(2^{\frac{n}{2}} + 1)$. Notice that $2^2 - 1 = 3^1$ but $2^4 - 1 = 15$ is not a power of 3. Thus, by induction (since every number is double a smaller even number or an odd number), there are no other solutions for n, m.

- $3^n - 1 = 2^m$ for integers n, m. We use a similar argument to before: if n is odd, $3^n - 1 \equiv (-1)^n - 1 = -1 - 1 \equiv 2 \pmod 4$. The only 2 mod 4 power of 2 is $2 = 3^1 - 1$. If n is even, $3^n - 1$ is only a power of 2 if $3^{\frac{n}{2}} - 1$ is a power of 2. We see $3^2 - 1 = 2^3$ but $3^4 - 1 = 80$ is not a power of 2, so by induction no other numbers work.

Thus we have found $(1, 2)$, $(3, 4)$, $(2, 3)$ and $(8, 9)$ as the only consecutive integer powers of 2 and 3.

10. For prime p, q, how many quadratic residues are there under mod pq?
Solution: You can prove this nicely by considering $a^2 \equiv b^2 \pmod{pq}$ and then considering when there are only 4, 2, or 1 unique solution(s) for b (try proving there can't be 3 unique solutions!), but I won't do that :D.

The space of mod pq is isomorphic to the group product of mod p and mod q (this roughly means that we could create a one-to-one mapping between every element in mod pq and a vector with the first row being an element from p and the second an element from q, and, more importantly, addition and multiplication and preserved as component-wise addition and multiplication). This means every quadratic residue can be found by taking all possible choosings of one quadratic residue from mod p and one from mod q (order preserved), which is $\frac{p+1}{2} \times \frac{q+1}{2} = \frac{(p+1)(q+1)}{4}$.

11. Prove there are infinite primes 1 mod 4. (a lot harder)
Solution: We will use question 8. Suppose there are finite number of 1 mod 4 primes, call them $p_1, p_2, \ldots, p_n$. Then, $4(p_1 p_2 \ldots p_n)^2 + 1 \equiv 1 \pmod 4$. This means, if we take a prime p that divides this equation, then because there exists $x = 2p_1 p_2 \ldots p_n$ such that $x^2 + 1 \equiv 0 \pmod p$, $p \equiv 1 \pmod 4$. However, $x^2 + 1 \equiv 0 + 1 = 1 \not\equiv 0 \pmod{p_i}$ for all $1 \leq i \leq n$, so p cannot be any of $p_1, \ldots, p_n$. Thus we have generated a new prime, resulting in a contradiction. This means there are infinite 1 mod 4 primes.