11/2 Fall 2022, Number Theory I Test II solutions Sitaraman

Howard University Math Department

PLEASE STUDY CLASS NOTES, HW PROBLEMS AND PRACTICE PROBLEMS IN ADDITION TO THESE.

1. (20 points) Explain which of the following statements are true and why. If false, give a counterexample.

   (a) Let a, m be nonzero integers, and $gcd(a, m) = 1$. Then $ax \equiv 1 \pmod{m}$ always has a solution. In other words, a^{-1} always exists in $(\mathbb{Z}/m\mathbb{Z})^*$.

   (b) $x^3 \equiv 2 \pmod{5^k}$ has a solution for any $k > 1$. In other words, $\sqrt[3]{2}$ always exists in $(\mathbb{Z}/5^k\mathbb{Z})^*$.

   (c) If $a^{n-1} \equiv 2 \pmod{n}$ for some $0 < a < n$, then n is composite.

   (d) The sum of all elements in $\mathbb{Z}/m\mathbb{Z}$ equals 0 mod m for all odd $m \in \mathbb{Z}$.

   Solution: They are all true!

   (a) Satisfies conditions for existence of solutions.

   (b) $\phi(5^k) = 4(5^{k-1}) \implies gcd(3, \phi(5^k)) = 1; gcd(2, 5^k) = 1$. So it satisfies all conditions for the existence of cube root. In fact, since $3y \equiv 1 \pmod{\phi(5^k)}$ has a solution, we have 2^y as the required solution. Check: $(2^y)^3 = 2^{3y} \equiv 2 \pmod{5^k}$.

   (c) True because if n were prime then by Fermat's little theorem $a^{p-1} \equiv 1 \pmod{p}$ for all $0 < a < n$.

   (d) True because $m/2 \notin \mathbb{Z}/m\mathbb{Z}$ there won't be any element of order 2.

2. (20 points) For each of the following give an example.

   (a) $(\mathbb{Z}/m\mathbb{Z})^*$ of order 4 in which none of the elements have order 4.

   (b) $m = pq$ where p, q are prime such that $(\mathbb{Z}/m\mathbb{Z})^*$ has a primitive root (i.e, it is a cyclic group).

   Solution:

   (a) $m = 8$ works. $(\mathbb{Z}/8\mathbb{Z})^*$ has order 4 but we have $3^2 = 9, 5^2 = 25, 7^2 = 49$ and all are 1 mod 8. So they all have order 2.

   (b) $m = 6$ works. In $(\mathbb{Z}/6\mathbb{Z})^*$ we only have two elements 1 and 5 and the group is generated by 5.

3. (20 points) State the prime number theorem giving the estimate for $\pi(x)$, the number of primes less than x. Use it to estimate the ratio $\pi(x)/\pi(x/2)$ as $x \to \infty$ and the ratio $\pi(x)/\pi(\sqrt{x})$ as $x \to \infty$.

Solution:

The prime number theorem says

$$\pi(x) \sim \frac{x}{\ln x} \; as \; x \to \infty.$$

Putting $x/2$ instead of x we get

$$\pi(x/2) \sim \frac{x/2}{\ln(x/2)} = \frac{x}{2\ln x - 2\ln 2} \sim \frac{x}{2\ln x} \; as \; x \to \infty.$$

So there are about half the number of primes below $x/2$ as x gets bigger.

Putting $\sqrt{x}$ instead of x we get

$$\pi(\sqrt{x}) \sim \frac{\sqrt{x}}{\ln(\sqrt{x})} = \frac{\sqrt{x}}{(1/2)\ln x} \sim \frac{2\sqrt{x}}{\ln x} \; as \; x \to \infty.$$

Dividing this in $x/\ln x$ we get the ratio $\pi(x)/\pi(\sqrt{x}) = \sqrt{x}/2$ as x gets bigger.

4. (20 points) Use the method of successive squaring to find $5^{23} \pmod{17}$.

   Solution:

   First we write $23 = 16 + 4 + 2 + 1 = 2^4 + 2^2 + 2^1 + 2^0$.

   Now we do successive squaring:

$$5^2 \equiv 8; 5^4 \equiv 8^2 \equiv -4; 5^8 \equiv (-4)^2 \equiv -1; 5^{16} \equiv 1.$$

   The last one we can also get from Fermat's little theorem.

$$So \; 5^{23} \equiv 5^{16+4+2+1} \equiv 1 \times (-4) \times 8 \times 5 = -32 \times 5 \equiv 10 \pmod{17}.$$

5. (20 points) Find $x \pmod{35}$ such that $x \equiv 2 \pmod 5$ and $x \equiv 3 \pmod 7$. Prove that this solution is unique.

   Solution:

   If $x \equiv 2 \pmod 5$ then $x \in \{2, 7, 12, 17, 22, 27, 32\}$. Among these we se that $17 \equiv 3 \pmod{17}$.

   The solution is unique, because, if x' is another solution, then $x' \equiv x \equiv 2 \pmod 5$ and $x' \equiv x \equiv 3 \pmod 7$. So 5 and 7 both divide $x - x'$ which means that 35 divides it. So $x' \equiv x \pmod{35}$. In other words, mod 35 there is only one solution.

6. (Bonus 20 points) Three men and a monkey were shipwrecked on an island. They spent the first day gathering coconuts. During the night, one man woke up and decided to take his share of the coconuts. He divided them into three equal piles. One coconut

was left over so he gave it to the monkey, then hid his share, put the remaining two-thirds back together, and went back to sleep. Soon the second man woke up and did the same thing. After dividing the coconuts into three piles, one coconut was left over which he gave to the monkey. He then hid his share, put the remaining two-thirds back together, and went back to bed. Then the third man did the same. In the morning they divided the remaining coconuts into three equal piles and none were left over. What is the smallest number of coconuts that could have been in the original pile? You must use congruences.

Solution: Let N be the initial number. Then after first division we are left with $2(N-1)/3$. After second division we are left with

$$\left(\frac{2(N-1)}{3} - 1\right)\frac{2}{3} = \frac{4N-10}{9}$$

After third division we are left with

$$\left(\frac{4N-10}{9} - 1\right)\frac{2}{3} = \frac{8N-38}{27}$$

Since the last pile was divisible into 3 piles, we get

$$\frac{8N-38}{27} = 3m \implies 8N - 38 = 81m \implies 8N \equiv 38 \pmod{81}$$

Since $gcd(8, 81) = 1$, this has a unique solution under 81. In fact, we have $(-10)8 + 1(81) = 1$. Multiplying by 38 we get $38(81) - (380)8 = 38$. Now $-380 = -56 \equiv 25 \pmod{81}$ so $25(8) \equiv 38 \pmod{81}$. The smallest N is 25.

Check: After first division, 16 are left. After second, 10 are left. After third, 6 are left. So each gets 2 in the end.