12/2 Fall 2022, Number Theory I Test III solutions Sitaraman

Howard University Math Department

TOTAL 100 POINTS.

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

   (a) If $n-1$ is a product of the form $(p_1-1)(p_2-1)...(p_k-1)$ where the p_i are distinct primes, then n is a Carmichael number.

   False. $8 = 2 \times 4$ but 9 is not a Carmichael number.

   (b) Every quadratic equation with integer coefficients has a solution mod any prime p.

   False. Even $x^2 + 1 = 0$ doesn't have solution mod any prime that is 3 mod 4.

   (c) 5 has a square root mod 19.

   True, using Legendre symbol formula. $5^9 \equiv 1 \pmod 9$.

   (d) The number of quadratic residues is always equal to number of quadratic non-residues mod p, if p is a prime.

   True. See text / notes.

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

   (a) A composite number n that is NOT a Carmichael number and $a > 1$ such that $a^n \equiv a \pmod n$.

   An easy example is $n-1$ which is -1 mod n. If n is odd we get $(-1)^n \equiv -1$. Slightly harder is $6^{10} \equiv 6 \pmod{10}$.

   (b) A prime p such that 3 has a square-root mod p.

   3 has a square root mod 11.

3. (20 points) State the Miller-Rabin test and explain why it works. Use it to show that 21 is composite.

   Solution: $21 - 1 = 20 = 4(5)$. So we look at a^5, a^{10} for some a not divisible by 21. Here we can take $a = 2$. Then we get $2^5 = 32 \equiv 11$ mod 21, $2^{10} \equiv 11^2 \equiv 121 \equiv -5$ mod 21. So 21 must be composite.

4. (20 points) Calculate the Legendre symbol of the following mod 23: 2, 3, 4, 5.

   Solution: 4 is a square, so it is a residue.

   2 is a residue because 23 is 7 mod 8.

   $3 \equiv 7^2$ mod 23, so it is a residue.

   $5^{11} \equiv ?$ mod 23 ? $5^2 \equiv 2$ mod 23, so $5^4 \equiv 4, 5^8 \equiv 16, 5^{10} \equiv 32 \equiv 9, 5^{11} \equiv 45 \equiv -1$ so 5 is not a residue.

5. (20 points) Show that, if -1 is not a residue mod an odd prime p then every non-residue is the negative of a residue mod p. Then show, for the non-residues n_i,

$$\sum_{k=1}^{P} k^2 \equiv p\left(\frac{p-1}{2}\right) - \sum_{i=1}^{P} n_i \pmod{p}, \ with \ P = \frac{p-1}{2}.$$

Finally show that, in this case, $p(p-1)/2$ is odd, and so the sum of the squares mod p and the sum of the non-squares mod p will be different.

Solution: If -1 is a non-residue, then $-k^2$ is a non-residue because a non-residue times a residue is a non-residue. Once you reduce the k^2 mod p and get the r_i, write $p - n_i = r_i$ for $i = 1, 2, ..., P$ where r_i are the squares mod p. Adding up, we get the result. Finally, when -1 is a non-residue, $p \equiv 3 \pmod 4$ and so $p(p-1)/2$ is odd. Because actually we have $\sum_{k=1}^{P} r_i + \sum_{i=1}^{P} n_i = p\left(\frac{p-1}{2}\right)$ the two sums cannot be equal because otherwise $p(p-1)/2$ has to be even.

6. (extra credit 20 points) Show that $5^{(p-1)/2} \not\equiv 1 \pmod p$ if $p \equiv 2 \pmod 5$.

Look at the product $(5)(10)(15)....(5P)$ where $P = (p-1)/2$.

As we did with the Legendre symbol for 2 we reduce the numbers $5, 10, 15, ...$ mod p and see how many are bigger than P. The number of $5k$ that are between P and $2P = p-1$ is the number of sign changes (again using the language from the proof for 2).

If $5k > P$ then $k > P/5 = (p-1)/10$. If $p \equiv 2 \pmod 5$ then $(p-2)/5$ is an integer because $p-2$ is divisible by 5. It is also odd because p is odd and so $p-2$ is odd. That means $\frac{p-2}{5} + 1 = (p+3)/5$ is even, thus $(p+3)/10$ is an integer which we call m. Then $5m = (p+3)/2 > P$ but $5(m-1) = (p-7)/2 < P$.

So $5m, 5(m+1), 5(m+2), ..., 5(2m-1)$ all are bigger than P and hence the negative of a number in $1, 2, ..., P$.

The following lines show which ones would become negative when reduced mod p and arranged in $(-(p-1)/2, (p-1)/2))$:

$$5(m-1) = \frac{p-7}{2} < \frac{p-1}{2} < \frac{p+3}{2} = 5m. \tag{1}$$

$$5(2m-1) = 10m - 5 = p - 2 < p - 1 < p + 3 = 10m. \tag{2}$$

$$15m - 5 = 5(3m-1) = 5(2m) + 5(m-1) = p + 3 + \frac{p-7}{2} = p + \frac{p-1}{2}$$
$$< 15m = p + \frac{p-1}{2} + 5 = p + \frac{p+9}{2}. \tag{3}$$

$$5(4m-2) = 15m + 5(m-1) - 5 = p + \frac{2p+2}{2} - 5 = 2p - 4$$
$$< 5(4m-1) = 5(4m-2) + 5 = 2p - 4 + 5 = 2p + 1. \tag{4}$$

$$5(5m-2) = 5(4m-1) + 5(m-1) = 2p + 1 + \frac{p-7}{2} = 2p + \frac{p-5}{2} < 2p + \frac{p-1}{2}. \quad (5)$$

$$But\ 5(5m-2) = 5\left[5\left(\frac{p+3}{10}\right) - 2\right] = 5\left(\frac{p-1}{2}\right).$$

So we have covered 5 times the whole set from 1 to $P = (p-1)/2$. Now we count how many end up between P and p after reducing mod p. We see that the total of such numbers from the 5 equations equals m from (2) plus $m-1$ from (4) and thus a total of $2m-1$. Thus the total number of sign changes is $2m-1$ and it is odd, so $5^{(p-1)/2} \equiv (-1)^{2m-1} = -1$.