11/29 Fall 2024, Number Theory I Final exam practice problems Sitaraman

**Howard University Math Department**

PLEASE STUDY CLASS NOTES, HW PROBLEMS AND TEST 1 AND 2 SOLUTIONS AND PRACTICE PROBLEMS IN ADDITION TO THESE.

1. Explain which of the following statements are true and why. If false, give a counterexample.
   (a) Every Carmichael number is a product of exactly three prime numbers
   (b) For every prime $p$ dividing $n$ if $p-1$ divides $n-1$ then $n$ is a Carmichael number.
   (c) $a^n \equiv a \pmod{n}$ for all $a < n$, for any integer $n$.
   (d) If $gcd(b, m) = gcd(k, \phi(m) = 1$ then $x^k = b$ has exactly one solution.
   (e) $2^n + 3$ is always a prime if $n > 0$.
   (f) If $am + bn = d$ then $d = gcd(m, n)$ where $a, b$ are integers.
   (g) $x^3 + 1 = 0$ can have 4 roots mod some prime.
   (h) The set of squares mod $p$ form a subgroup of $\mathbb{F}_p^*$.
   (i) If an integer $n$ divides $ab$ then it divides either $a$ or $b$.
2. For each of the following give an example.
   (a) A composite number $n$ such that $a^n \equiv a \pmod{n}$ for all $a \leq n$.
   (b) A linear congruence relation $ax \equiv b \pmod{m}$ that has no solutions.
3. Use the method of successive squaring to find $3^{51} \pmod{11}$. Compare your answer with what you get using Fermat's Little Theorem.
4. Describe all integer solutions for $3x + 4y = 1$.
5. (Slightly harder) Given any integer $a$, can you find integers $b, c$ that form a Pythagorean triple with $a$, i.e, $(a, b, c)$ is a Pythagorean triple ? Prove if true, disprove if false.
6. For what $c$ would $4x + 6y = c$ NOT have solutions?
7. Describe the GCD and LCM of two numbers in terms of their prime factors.
8. Show that $x(x + 1)(x + 2) = 3m$ for some integer $m$ for all integers $x > 0$.
   [Hint: Look at remainders mod 3].
9. Problems from Chapter 13 (please read by yourself – it is survey)
   1. Show that the numbers $n! + 2, n! + 3, ...., n! + (n - 1), n! + n$ are all composite for any integer $n \geq 2$.
   2. Will there be infinitely many primes of the form $n^3 + 1$?

10. Solve $x^{329} \equiv 452 \pmod{1147}$ (Note: 1147 is not prime).

11. (Problem 17.4) Show that the method to find $k$-th root of an integer $b$ mod $m$ works even if $m$ is a product of primes, as long as each prime divides $m$ only once. [Hint: Write $b = b' \times gcd(b, m)$ where $gcd(m, b') = 1$. Then use chinese remainder theorem].

12. (Problem 18.2b – Please read chapter 18, it is also a survey) Show that RSA decryption works for all messages $a$ as long as $m$ is a product of distinct primes.

13. Why cannot we use the same method (as in 17.4) to find the square root of 23 mod 1279?

14. Show that there are infinitely many primes that are congruent to 5 mod 6.

15. Show that, if $a^n + 1$ is prime for some numbers $a \geq 2, n \geq 1$ then $n$ must be a power of 2 and $n = 2$.

16. Problems from chapter 15:

    1. If $m, n$ are integers with $gcd(m, n) = 1$, show that $\sigma(mn) = \sigma(m)\sigma(n)$.

    2. Calculate $\sigma(20)$ and $\sigma(1728)$.

    3. Show that if $p, q$ are distinct odd primes then a number of form $p^i q^j$ cannot be perfect.

    4. Show that a square number cannot be perfect.