MA222: Elementary Number Theory and Algebra

Instructor: Anupam Saikia

Assignment 2: Diophantine Equations, Congruence, Fermat's Little Theorem

---

1. Find all the solutions of the linear congruence $18x \equiv 12 \pmod{30}$.

2. Find the largest four digit integer that leaves remainder 7 when divided by 15, remainder 3 when divided by 7 and remainder 5 when divided by 8.

3. Show that here are infinitely many positive integers which cannot be expressed as sum of three squares.

4. Prove that there are infinitely many positive integers which are not representable as a sum of cubes of two other positive integers.

5. Show that $x^3 + y^3 = z^3$ with $3 \nmid xyz$ has no solutions in integers.

6. Show that
$$1! + 2! + 3! + \ldots + n!$$
is a perfect square if and only if $n = 3$.

7. If $gcd(a, 30) = 1$, show that 60 divides $a^4 + 59$.

8. Let p be a prime of the form $3k + 2$ that divides $a^2 + ab + b^2$ for some natural numbers a and b. Show that a and b are both divisible by p.

9. Consider the sequence given recursively as $a_n = 100a_{n-1} + 134$, $a_1 = 24$, $a_2 = 2534, \ldots$. Determine the smallest n such that $99 \mid a_n$.

10. Show that 561 is a pseudoprime (to the base 2).

11. Show that 91 is a pesudoprime to the base 3.

12. Show that 1105 is a Carmichael number.

13. Using Chinese Remainder Theorem, show that a Carmichael number must be square-free.

14. Consider a composite square-free number $n = p_1 p_2 \cdots p_r$ (where p_i are distinct primes). Show that n is a Carmichael number if $(p_i - 1) \mid (n - 1)$ for $i = 1, 2, \ldots r$.

15. Prove that any integer of the form $n = (6k+1)(12k+1)(18k+1)$ is a Carmichael number if $6k + 1$, $12k + 1$ and $18k + 1$ are all primes.

16. (a) If p is an odd prime not dividing $a^2 - 1$, then show that $m = \frac{a^{2p}-1}{a^2-1}$ is a pseudoprime to the base a. (*Start with Fermat's Little Theorem to show that* $p \mid (m - 1)$. *You need to prove and use* $2p \mid (m - 1)$).

    (b) Deduce that there are infinitely many pseudoprimes to any given base a.

****