EE720: Problems on division, groups, extended Euclidean, CRT, Fermat and Euler theorems

January 25, 2015

Solve the problems using SAGE or if explicitly mentioned, using calculators. SAGE demo will be given in class. Can be used directly on the net at cloud.sagenb.org after registering yourself. Do inform course instructor if the numbers are large enough to be computed in SAGE.

1. Show that a decimal number $a_1a_2\ldots a_n = (a_1 + a_2 + \ldots + a_n) \mod 9$. For example $738864 = (7 + 3 + 8 + 8 + 8 + 6 + 4) \mod 9$. Using this solve the following without using a calculator
   (a) Show that $123456789123456789 + 234567891234567891 \neq 358025680358025680$
   (b) Show that
   $$123456789123456789 \times 234567891234567891 \neq 28958998683279996179682996625361999$$

2. Using only calculator with no more than 12 digit display find the exact integer product
   $$4444555566669 \times 1111222233338$$

3. Solve without calculator. Show that $39|53^{103} + 103^{53}$, $7|111^{333} + 333^{111}$. (Appeared in IB 12th class exam).

4. Show that $7|5^{2n} + 3 \times 2^{5n-2}$, $13|3^{n+2} + 4^{2n+1}$, $27|2^{5n+1} + 5^{n+2}$, $17|11^{104} + 1$ without using calculators. (Appeared in IB 12th class exam).

5. Find $(\sum_{j=1}^{100} j^5) \mod 4$.

6. For $m = 67862310031$ find $x = 2^{-1} \mod m$. If $n = 1 \mod b$, what integer between 1 and $n - 1$ equals $b^{-1} \mod n$?

7. If g is an integer such that $g^a = 1 \mod m$ and $g^b = 1 \mod m$ then show that $g^{\gcd(a,b)} = 1 \mod m$.

8. Find whether following equations are solvable and find all solutions when they exist. Give reasons if they dont exit.

(a) $122X = 1 \mod 343$.

(b) $(2^{27} - 1)X = 7^3 \mod 2^{21} - 1$.

(c) $(193707721)X = 1 \mod 761838257287$.

9. Solve the linear equation $aX + bY = c$ for given a, b, c. Find the solution X which is the smallest positive integer.

   (a) $a = 765355768$, $b = 76354890023$, $c = 863429$

   (b) $a = 2^{100} - 1$, $b = 2^{102} - 1$, $c = 6442450941$

   (c) $a = 3014774729910783238001$, $b = 15733624667337520130581$. Find at least three integers c for each of which there are solutions. Find these solutions.

10. Solve the following simultaneous congruances or explain why there is no solution.

    (a) $X = 37 \mod 43$, $X = 22 \mod 49$, $X = 18 \mod 71$.

    (b) $X = 3 \mod 299593$, $X = 2 \mod 19173961$, $(54525951)X = 2 \mod (2^{22} - 1)$.

    (c) $X = 133 \mod 451$, $X = 237 \mod 697$.

11. Find the order of a in $\mathbb{Z}_n^*$ for given a, n.

    (a) $a = 5$, $n = 2^{202} - 1$.

    (b) $a = 5342$, $n = 2^{200} - 1$.

    (c) $a = 2222574487$, $n = 7$.

12. Given prime factorization $n = 41^3 \times 101^3 \times 251^2$ find $3^{72549625} \mod n$ using the CRT.

13. Use CRT to find $2^{477} \mod 1000$, $11^{507} \mod 1237$.

14. If p is prime what are orders of all subgroups of $\mathbb{Z}_p^*$? Find a primitive element of $\mathbb{Z}_p^*$ for the prime number $p = 87449423397425857942678833145441$ by trial and error and then using factorization of $p - 1$. Find generators of all cyclic subgroups of all orders of $\mathbb{Z}_p^*$.

15. Show that if $n = pq$ for primes p, q and $d = \gcd(p - 1, q - 1)$ then for any a coprime to n, $a^{\phi(n)/d} = 1 \mod n$.