EE720: Problem Set 2.2: Euclidean division, groups, CRT, Fermat and Euler theorems

February 2, 2017

Solve the problems using SAGE or Maple or using calculators. SAGE can be used directly on the net at cloud.sagenb.org after registering yourself. Similarly Maple is available on your LDAP Id.

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

   $$123456789123456789 \times 234567891234567891 \neq 28958998683279996179682996625361999$$

   Hint: Write the decimal number as $a_n + a_{(n-1)} * 10 + \ldots + a_1 * 10^n$. Calculate each term modulo 9.

   Hint: Take sum of digits in each number modulo 9. Then the sums on LHS and RHS must match if the two sides are equal. Similarly take product modulo 9 of sums of digits of each number. If the product is same the product modulo 9 must match.

2. Using only calculator with no more than 12 digit display find the exact integer product

   $$4444555566669 \times 1111222233338$$

   Hint: Number of digits are 13. Express the numbers is expansion in terms of a base $B = 10^6$. Then find the expansion in base B of the form $a_0 + a_1 * B + a_2 * B^2 + a_3 * B^3$. Write an expression of product expanded in B. The product will involve carry digits and expansion upto degree B^6. Compute the co-efficients of product from the expansion co-efficients of original numbers on the calculator. They will involve numbers less than 12 digits.

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

   Hint: n divides a^b is equivalent to $a^b \mod n = 0$. Hence compute $a^{(b \mod \phi(n))} \mod n$ and test whether it is zero.

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).

   Hint: Just try it is high school problem.

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

   Hint: High school.

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

   Hint: You need to solve x such that $x2 \mod m = 1$ since m is odd it is coprime to 2 hence there exist x, y such that $2x + my = 1$ by extended Euclid. For the next one think on same lines.

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

   Hint: Order of g divides both a, b. Hence order g divides their gcd.

8. Problems on p-adic expansion. Denote by $(a_0, a_1, \ldots, a_{m-1})_p$ the positive integer

$$a = \sum_{i=0}^{m-1} a_i p^i$$

   Carry out by high school method 1) $(101101)_2 \times (1110011)_2$, 2) $(50AB89F)_{16} \times (879CD)_{16}$, 3) $(4400327)_8 \div (5763)_8$, 4) Write last two digits of 11-adic expansion of the decimal number 87900547, 5) write the number $(3402133)_5$ as an octal number.

   Hint: High school.

9. 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) $(193707721)X = 1 \mod 761838257287$.

   Hint: Use extended Euclidean division.

10. 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.

    Hint: Solve first the identity $ax + by = d$ where d is gcd of a, b. The solution exists iff $d|c$. From the multiplier find one solution X, Y. Assume other solutions X', Y' and find in terms of X, Y.

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

    Hint: Straightforward application of CRT.

12. 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) $a = 2222574487$, $n = 7$.

    Hint: Some numbers might be too large for the calculator. You can use smaller exponents of 2 and resolve the problem. Find prime factorization of $\phi(n)$ using SAGE.

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

    Hint: Already given, use CRT.

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

    Hint: Already given.

15. 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 $\mathbb{Z}_p^*$.

    Hint: The number p might be too large even for SAGE. Take a smaller p and solve. Use the order computation algoroithm discussed in class149.

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

    Hint: Solve on your own.