

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.sagemath.org after registering yourself. Similarly Maple is available on your LDAP Id.

1. Show that a decimal number $a_1a_2 \dots a_n = (a_1 + a_2 + \dots + a_n) \pmod 9$. For example $738864 = (7 + 3 + 8 + 8 + 8 + 6 + 4) \pmod 9$. Using this solve the following without using a calculator

(a) Show that $123456789123456789 + 234567891234567891 \neq 358025680358025680$

(b) Show that

$$\begin{aligned} 123456789123456789 \times 234567891234567891 &\neq \\ 28958998683279996179682996625361999 &\end{aligned}$$

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 $(\sum_{j=1}^{100} j^5) \pmod 4$.
6. For $m = 67862310031$ find $x = 2^{-1} \pmod m$. If $n = 1 \pmod b$, what integer between 1 and $n - 1$ equals $b^{-1} \pmod n$?
7. If g is an integer such that $g^a = 1 \pmod m$ and $g^b = 1 \pmod m$ then show that $g^{\gcd(a,b)} = 1 \pmod m$.
8. Problems on p -adic expansion. Denote by $(a_0, a_1, \dots, a_{m-1})_p$ 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.

9. Find whether following equations are solvable and find all solutions when they exist. Give reasons if they don't exist.
 - (a) $122X = 1 \pmod{343}$.
 - (b) $(2^{27} - 1)X = 7^3 \pmod{2^{21} - 1}$.
 - (c) $(193707721)X = 1 \pmod{761838257287}$.
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.
11. Solve the following simultaneous congruences or explain why there is no solution.
 - (a) $X = 37 \pmod{43}, X = 22 \pmod{49}, X = 18 \pmod{71}$.
 - (b) $X = 3 \pmod{299593}, X = 2 \pmod{19173961}, (54525951)X = 2 \pmod{(2^{22} - 1)}$.
 - (c) $X = 133 \pmod{451}, X = 237 \pmod{697}$.
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) $a = 2222574487, n = 7$.
13. Given prime factorization $n = 41^3 \times 101^3 \times 251^2$ find $3^{72549625} \pmod{n}$ using the CRT.
14. Use CRT to find $2^{477} \pmod{1000}, 11^{507} \pmod{1237}$.
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^* .
16. Show that if $n = pq$ for primes p, q and $d = \gcd(p - 1, q - 1)$ then for any a coprime to n , $a^{\phi(n)/d} = 1 \pmod{n}$.