THE UNIVERSITY OF BRITISH COLUMBIA

Math 312 Section 951

Calculators are allowed
No cell phones or information sheets allowed
Exam length is 2 hours and 30 minutes

FINAL EXAM

August 15, 2023

NAME

STUDENT NUMBER

1(a) Find the smallest positive integer with exactly 15 positive divisors.
(b) Find all integers > 1 such that $\phi(n) = 12$, where ϕ is the Euler phi function.

$15 = 3 \times 5$ ~~$15 = 1 \times 3 \times 5$~~

$15 = 15$

$p_1^2 p_2^4$

p_1^{14}

$3^2 2^4 = 9 \times 16 = 144$

~~$\phi(n) =$~~

~~$\phi(n) = 3 \times 4 = (1+3)(1+3)$~~

$\phi(n) = 12$

$= (2-1) \times 12$

$= 2^2 \times 3$

$= 2 \times 3 \times 2$

$= 2 \times 6$

$= (3-1) \times (7-1)$

$= (2-1)(3-1) \times (7-1)$

$= 2(2-1) \times (7-1)$

$n = 13$ ①

$n = 26$ ②

$n = 2^2 \times 3^2$

$= 4 \times 9 = 36$ ③

$n = 3 \times 7 = 21$ ④

$n = 42$ ⑤

$n = 2^2 \times 7 = 28$ ⑥

2. Show that if $c_1, c_2, \ldots, c_{\phi(m)}$ is a reduced residue system mod m, where m is a positive integer not equal to 2, then $c_1 + c_2 + \ldots + c_{\phi(m)} \equiv 0 \pmod{m}$.

$c_1 \quad m - c_1$

$(c_1\ m) = 1$

$= (c_1\ m - c_1) = 1$

3. (a) Show that 2047 passes Miller's test to the base 2.
   (b) Prove that 2821 is a Carmichael number.

$$2^{2047-1} \equiv 1 \pmod{\cancel{A}\ 2047}$$

$$2^{10} = 1024$$

$$2^{11} = 2048 \equiv +1 \mod 2047$$

$$2^{2046} = 2^{11 \times 186} \equiv 1 \mod 2047$$

$$2046 = 11 \times \cancel{2\times 93}\ 3 \times 2 \times 31$$

$$2^{1023} = 2^{93 \times 11} \equiv 1 \mod 2047$$

$$2821 = 7 \times 403$$
$$= 7 \times 13 \times 31$$

2821 is square free.

Korselt's criterion

~~2821~~ $6 \mid 2820$

$12 \mid 2820$

$30 \mid 2820$

4. The Indian astronomer and mathematician Mahavira, who lived in the ninth century, posed this puzzle: A band of 23 weary travellers entered a lush forest where they found 63 piles each containing the same number of plantains and a remaining pile containing 7 plantains. They divided the plantains equally. How many plantains were in each of the 63 piles? Find the smallest solution.

$63x + 7 = 23n$

63

126+7

133

$63 = 23\times 2 + 17$

$23 = 17\times 1 + 6$

~~17 = 6×3 + 2~~

~~6 = 2×2 + 1~~

$17 = 6\times 2 + 5$

$6 = 5\times 1 + 1$

$1 = 6 - 5\times 1$

$= 6 - (17 - 6\times 2)\times 1$

$= 6\times 3 - 17\times 1$

$= (23 - 17\times 1)\times 3 - 17\times 1$

$= 23\times 3 - 17\times 4$

$= 23\times 3 - (63 - 23\times 2)\times 4$

$= 23\times 11 - 63\times 4$

$1 = 5 - 2\times 2$

$= 5 - (17 - 5\times 3)\times 2$

$= -17\times 2 + 5\times 7$

$= -17\times 2 + (23 - 17\times 1)\times 7$

$= -17\times 9 + 23\times 7$

$= -(63 - 23\times 2)\times 9 + 23\times 7$

$= -63\times 9 + 23\times 25$

$7 = 23\times 77 - 63\times 28$

$= 23\times(77 + 63\times 9) - 63\times(28 + 23\times ...)$

$= 23\times 14 - 63\times 5$

5. Use Euler's theorem to find the least positive residue of 2^{94338}(mod 77). Alternatively, you may use the Chinese Remainder Theorem.

~~$2^{76} \equiv 1$ (m~~

$\phi(77) = \phi(7)\phi(11)$
$= 6 \times 10 = 60.$

$2^{60} \equiv 1 \pmod{77}$

$94338 = 60 \times 1572 + 18$

$$\begin{array}{r} 1572 \\ 60\,\overline{)94338} \\ 60 \\ \hline 343 \\ 300 \\ \hline 433 \\ 420 \\ \hline 138 \\ 120 \\ \hline 18 \end{array}$$

$2^{94338} = 2^{1572 \times 60 + 18} = 2^{18} \pmod{77}$

$2^{6} = 64 = -13 \bmod 77$

$(-13)^{3} \bmod 77$

$13 \times 13 = 169$
154
$(-13)^{2} \equiv 15 \pmod{77}$
$-15 \times 13 = -195$

$-195 + 77 \times 3$
$= -195 + 231$
$= 36.$

6. Show that $a^{\phi(b)} + b^{\phi(a)} = 1 \pmod{ab}$, if a and b are relatively prime positive integers and ϕ is the Euler phi function.

$a^{\phi(b)} \equiv 1 \mod (b)$

$b^{\phi(a)} \equiv 1 \mod a$

$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod a$

$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod b$

$\Downarrow$

...

7. (a) Determine whether 63 is a pseudoprime to the base b = 2.
   (b) Determine whether 1387 is a strong pseudoprime to the base b = 2

In both parts please show your reasons.

(a) $\cancel{2^{63}}$ $2^{62} \bmod (63)$

$= (2^6)^{10} \cdot 2^2 \equiv (-1)^{10} \cdot 4 \pmod{63}$

$= 4 \bmod 63$

(b) 2^{1386} ~~mod~~

$= 2.$

$1386 = 2 \times 693$

$= 2 \times 3 \times 231$

$= 2 \times 3^2 \times 7 \times 11$

$2^{3^2 \times 7 \times 11} \bmod 1387$ 2048 ~~661~~

$(661)^{3^2 \times 7} \bmod 1387$

$= 512 \bmod 1387$

$2^{11} = 2048$

$= 661 \bmod 1387$

8. Show that every nonzero integer can be uniquely expressed as

$$a_k 3^k + a_{k-1} 3^{k-1} + \dots a_1 3 + a_0$$

Where each a_i is -1 or 0 or 1 and a_k is not 0.

$n \bmod 3.$

$[0] \quad [1] \quad [2]$

$n_0 \in [0] \quad a_0 = 0 \quad n_i = \frac{n_0}{3}$

$n_0 \in [1] \quad a_0 = 1 \quad n_i = \frac{n_0 - 1}{3}$

$n_0 \in [2] \quad a_0 = -1 \quad n_i = \frac{n_0 + 1}{3}$

9. (a) Give the definition of primitive root and find and prove that you have found a primitive root of 29.

$2 \quad \phi(28)$

(b) How many incongruent roots of 29 are there? Justify your answer.

(c) If possible, find a primitive root of 34 and prove that it is primitive or show why such a root cannot be found.

$2^{28} \equiv 1 \mod 29$

$2^{14} \equiv (-3) \cdot 16 \mod 29 = 10 \mod 29$

$2^{7} \equiv (-3) \times 4 \mod 29 = 17 \mod 29$

$2^4 \equiv 16 \mod 29$

$2^2 \equiv 4 \mod 29$

$2^0 \quad \cdots \quad 2^{28}$

10. Suppose the message 04 23 00 12 has been received using the RSA encryption system with public key (n, e) = (33, 3).
    (a) Find the private (deciphering) key d and then
    (b) Decipher the message.

$a^{3\times \cancel{d}\,7} \equiv \cancel{x}\,a \pmod{33}$

$33 = 3\times 11$

$04^7 \bmod 33$

$\phi(33) = 2\times 10 = 20$

$a^{20} \equiv 1 \pmod{33}$

$3\times d = 20k+1$