Math 312: Midterm 2 Solutions

Problem 1

Find all solutions to

(a) $57x \equiv 87 \mod 105$

(b) $49x \equiv 5000 \mod 999$

1a. Using the Euclidean algorithm, we have

$$\begin{aligned} 105 &= 57 + 48 \\ 57 &= 48 + 9 \\ 48 &= (9)(5) + 3 \\ 9 &= (3)(3) + 0. \end{aligned}$$

Therefore $\gcd(57, 105) = 3 \mid 87$, and hence there are 3 incongruent solutions.

Using back substitution, we find

$$\begin{aligned} 3 &= 48 - (9)(5) \\ &= 48 - (57 - 48)(5) = (6)(48) - (57)(5) \\ &= (6)(105 - 57) - (57)(5) \\ &= (6)(105) + (-11)(57). \end{aligned}$$

It follows that $3 = (6)(105) + (-11)(57)$ and hence, multiplying by $\frac{87}{3} = 29$, we obtain

$$87 = 105(6 \cdot 29) + 57(-11 \cdot 29) = 105(174) + 57(-319).$$

Modulo 105, this is

$$57 \cdot (-319) \equiv 57 \cdot 101 \equiv 87 \mod 105.$$

In other words, $x_0 = 101$ is a solution to $57x \equiv 87 \mod 105$. Now, all other solutions are given by

$$x \equiv x_0 - \frac{105}{\gcd(57, 105)} t = 101 - 35t \mod 105, \qquad 0 \leq t \leq 2.$$

Now, all solutions are given by

$$x \equiv 101 \mod 105, \quad x \equiv 66 \mod 105, \quad x \equiv 31 \mod 105.$$

1b. Using the Euclidean algorithm, we have

$$\begin{aligned} 999 &= (49)(20) + 19 \\ 49 &= (19)(2) + 11 \\ 19 &= (11)(1) + 8 \\ 11 &= (8)(1) + 3 \\ 8 &= (3)(2) + 2 \\ 3 &= (2)(1) + 1 \\ 2 &= (1)(2) + 0. \end{aligned}$$

Therefore $\gcd(49, 999) = 1 \mid 5000$, and hence there is 1 incongruent solution.

Using back substitution, we find

$$\begin{aligned} 1 &= 3 - 2 = 3 - (8 - (3)(2)) = 3(3) - 8 \\ &= 3(11 - 8) - 8 = 3(11) - 4(8) \\ &= (3)(11) - 4(19 - 11) = (7)(11) - 4(19) \\ &= 7(49 - 19(2)) - 4(19) = 7(49) - 18(19) \\ &= 7(49) - 18(999 - (20)(49)) \\ &= (-18)(999) + (367)(49). \end{aligned}$$

It follows that $1 = (-18)(999) + (367)(49)$ and hence, multiplying by $\frac{5000}{1} = 5000$, we obtain

$$5000 = (999)(-18 \cdot 5000) + (49)(367 \cdot 5000) = (999)(-90000) + (49)(1835000).$$

Modulo 999, this is

$$49 \cdot 1835000 \equiv 49 \cdot 836 \equiv 5000 \mod 999.$$

In other words, $x_0 = 836$ is a solution to $49x \equiv 5000 \mod 999$. Now, all solutions are given by

$$x \equiv 836 \mod 105.$$

Problem 2

Find all integers x which satisfy all of the following congruences simultaneously

$$\begin{aligned} x &\equiv 1 \mod 4 \\ 2x &\equiv 3 \mod 5 \\ 4x &\equiv 5 \mod 7. \end{aligned}$$

(Hint: first solve each congruence for x and then use the Chinese Remainder Theorem.)

Problem 2 continued on next page...

Method 1.
Since $x \equiv 1 \mod 4$, we have that $x = 1 + 4k$ for some $k \in \mathbb{Z}$. Now, since $2x \equiv 3 \mod 5$, we have

$$2x \equiv 2(1 + 4k) \equiv 2 + 3k \equiv 3 \mod 5.$$

That is,

$$3k \equiv 1 \mod 5$$

so that $k \equiv 2 \mod 5$. Now, $k = 2 + 5l$ for some integer l. It follows that

$$x = 1 + 4k = 1 + 4(2 + 5l) = 9 + 20l.$$

Lastly, since $4x \equiv 5 \mod 7$, we have

$$4x \equiv 4(9 + 20l) \equiv 1 + 3l \equiv 5 \mod 7,$$

so $3l \equiv 4 \mod 7$. Solving this yields $l \equiv 6 \mod 7$ and hence

$$x = 9 + 20l = 9 + 20(6 + 7m) = 129 + 140m$$

for some integer m. That is

$$x \equiv 129 \mod 140.$$

Method 2. Solving

$$\begin{aligned} x &\equiv 1 \mod 4 \\ 2x &\equiv 3 \mod 5 \\ 4x &\equiv 5 \mod 7. \end{aligned}$$

is equivalent to solving

$$\begin{aligned} x &\equiv 1 \mod 4 \\ x &\equiv 3 \cdot 3 \equiv 4 \mod 5 \\ x &\equiv 5 \cdot 2 \equiv 3 \mod 7. \end{aligned}$$

Let $n_1 = 4, n_2 = 5$ and $n_3 = 7$. Now, let $m = n_1 n_2 n_3 = 140$. Since $4, 5, 7$ are pairwise coprime, the Chinese Remainder Theorem tells us that a unique solution modulo m exists. In particular,

$$x = b_1 m_1 y_1 + b_2 m_2 y_2 + b_3 m_3 y_3 \mod m,$$

where $b_1 = 1, b_2 = 4$ and $b_3 = 3$. Further, $m_i = m/n_i$ for $i = 1, 2, 3$ so that $m_1 = 140/4 = 35$, $m_2 = 140/5 = 28$, and $m_3 = 140/7 = 20$. Now, for $i = 1, 2, 3$ we have to solve $m_i y_i \equiv 1 \mod n_i$.

$$\begin{aligned} i = 1: &\quad 35y_1 \equiv 1 \mod 4 \implies y_1 \equiv 3 \mod 4 \\ i = 2: &\quad 28y_2 \equiv 1 \mod 5 \implies y_2 \equiv 2 \mod 5 \\ i = 3: &\quad 20y_3 \equiv 1 \mod 7 \implies y_3 \equiv 6 \mod 7. \end{aligned}$$

It follows that

$$x = (1)(35)(3) + (4)(28)(2) + (3)(20)(6) = 689 \equiv 129 \mod 140.$$

Problem 3

(a) Determine whether 209 passes Miller's test to the base 2.

(b) Determine whether 2821 is a Carmichael number.

3a. We must first determine whether 209 is a pseudoprime to the base 2. That is, we check whether

$$2^{208} \equiv 1 \mod 209.$$

Note that

$$208 = 2^7 + 2^6 + 2^4.$$

Using fast modular exponentiation, we find

$$\begin{aligned} 2^2 &\equiv 4 \mod 209 \\ 2^4 \equiv 4^2 &\equiv 16 \mod 209 \\ 2^8 \equiv 16^2 &\equiv 47 \mod 209 \\ 2^{16} \equiv 47^2 &\equiv 119 \mod 209 \\ 2^{32} \equiv 119^2 &\equiv 158 \mod 209 \\ 2^{64} \equiv 158^2 &\equiv 93 \mod 209 \\ 2^{128} \equiv 93^2 &\equiv 80 \mod 209. \end{aligned}$$

Now

$$2^{208} = 2^{2^7+2^6+2^4} = 2^{128} \cdot 2^{64} \cdot 2^{16} \equiv 80 \cdot 93 \cdot 119 \equiv 36 \mod 209.$$

It follows that 209 is not a pseudoprime to the base 2, and hence fails Miller's test.

3b. First observe that $2821 = 7 \cdot 13 \cdot 31$ so that 2821 is squarefree. Now, to appeal to Korset's criteria, we must show that for every $p \mid 2821$, we have that also $p - 1 \mid 2821 - 1$. Indeed

$$\begin{aligned} 7 \mid 2821, &\quad \frac{2820}{6} = 470 \\ 13 \mid 2821, &\quad \frac{2820}{12} = 235 \\ 31 \mid 2821, &\quad \frac{2820}{30} = 94. \end{aligned}$$

Therefore, by Korset's criteria, 2821 is a Carmichael number.

Problem 4

Let $\phi(x)$ be the Euler ϕ function.

(a) Find $\phi(945)$ and $\phi(144)$

(b) Find all integers such that $\phi(x) = 10$.

Problem 4 continued on next page...

4a.

$$\begin{aligned}\phi(945) &= \phi(3^3 \cdot 5 \cdot 7)\\ &= \phi(3^3)\phi(5)\phi(7)\\ &= (3^2)(3-1)(5)(6)\\ &= 432.\end{aligned}$$

Similarly,

$$\begin{aligned}\phi(144) &= \phi(2^4 \cdot 3^2)\\ &= \phi(2^4)\phi(3^2)\\ &= (2^3)(2-1)(3)(3-1)\\ &= 48.\end{aligned}$$

4b.
Suppose $x = p_1^{a_1} \cdots p_n^{a_n}$ such that $\phi(x) = 10$. By definition,

$$\phi(x) = \prod_{i=1}^{n} p_i^{a_i-1}(p_i - 1) = 10.$$

Suppose first that for some $i \in \{1, \ldots, n\}$, we have $p_i > 11$. Then $10 = \phi(x) \geq p_i - 1 > 11 - 1 = 10$, which is a contradiction. Hence, p_i must be among the primes $\{2, 3, 5, 7, 11\}$.

Suppose further that $p_i = 7$. Then $7^{a_i-1}(6) \mid 10$, which again is a contradiction, so that $p_i \neq 7$. Similarly, suppose that $p_i = 5$. Then $5^{a_i-1}(4) \mid 10$, which is a contradiction so that $p_i \neq 5$.

Now, we have $x = 2^a 3^b 11^c$. If $b \geq 2$, then $3^{b-1} \mid 10$, which is a contradiction, so $b \in \{0, 1\}$. Similarly, if $c \geq 2$, then $11^{c-1} \mid 10$, a contradiction. Hence $c \in \{0, 1\}$. Lastly, if $a \geq 3$, then $2^{a-1} \mid 10$, a contradiction, so $a \in \{0, 1, 2\}$.
Suppose in addition that $c = 0$ so that $x = 2^a 3^b$. Then $\phi(x) = 2^{a-1}3^{b-1}(3) = 10$, which is a contradiction as 5 clearly does not divide the left-hand-side. Hence $c = 1$. Now, checking all possibilities, we are left with

$$\begin{aligned}x = 2^0 3^0 11 = 11, &\implies \phi(x) = \phi(11) = 10\\ x = 2^1 3^0 11 = 22, &\implies \phi(x) = \phi(22) = 10\\ x = 2^0 3^1 11 = 33, &\implies \phi(x) = \phi(33) = 20\\ x = 2^1 3^1 11 = 66, &\implies \phi(x) = \phi(66) = 20.\end{aligned}$$

It follows that $x = 11, 22$ are the only integers such that $\phi(x) = 10$.

Problem 5

Suppose that one digit, indicated with a question mark, in each of the following ISBN10 codes has been smudged and cannot be read. What should this missing digit be? Show your work.

(a) $91-554-212?-6$

(b) $0-19-8?3804-9$

5a. For the code to be valid we need

$$\sum_{i=1}^{10} i\cdot a_i \equiv 0 \pmod{11} \iff 1\cdot 9+2\cdot 1+3\cdot 5+4\cdot 5+5\cdot 4+6\cdot 2+7\cdot 1+8\cdot 2+9\cdot ?+10\cdot 6\equiv 0 \pmod{11}$$

giving

$$9\cdot ? \equiv 4 \pmod{11} \iff ? \equiv 9 \pmod{11}.$$

5b. For the code to be valid we need

$$\sum_{i=1}^{10} i\cdot a_i \equiv 0 \pmod{11} \iff 1\cdot 0+2\cdot 1+3\cdot 9+4\cdot 8+5\cdot ?+6\cdot 3+7\cdot 8+8\cdot 0+9\cdot 4+10\cdot 9\equiv 0 \pmod{11}$$

giving

$$5\cdot ? \equiv 3 \pmod{11} \iff ? \equiv 5 \pmod{11}.$$