Math 373 — Practice Final Exam 2

Multiple Choice Section

(1) The number of integer solutions to the linear Diophantine equation $12x - 21y = 4$ is ______
   (A) 0  (B) 1  (C) 2  (D) 3  (E) infinite  (F) none of these.

Solution.  A.
Since $\gcd(12, -21) = 3$ which does not divide 4, so the equation has no integer solutions.

(2) If $a \equiv 4 \pmod{5}$ and $b \equiv 3 \pmod{5}$, then $2a + 3b \equiv \_\_\_\_ \pmod{5}$.
   (A) 0  (B) 1  (C) 2  (D) 3  (E) 4  (F) 5.

Solution.  C.
$2a + 3b \equiv 2 \times 4 + 3 \times 3 \equiv 8 + 9 \equiv 2 \pmod{5}$

(3) The inverse of 7 modulo 11 is ______
   (A) 1  (B) 3  (C) 8  (D) 9  (E) 10  (F) none of these.

Solution.  C.
(4) If \( m \) is an integer, then a complete residue system modulo \( m \) must consists of ______ numbers.

(A) 0  (B) 1  (C) \( m - 1 \)  (D) \( m \)  (E) \( m^2 \)  (F) none of these.

Solution.  D.

(5) Which of the following is NOT a complete residue system modulo 5?

(A) \{0, 1, 2, 3, 4\}  (B) \{6, 7, 8, 9, 10\}  (C) \{0, 5, 10, 15, 20\}

(D) \{3, 6, 9, 12, 15\}  (E) \{-2, -1, 0, 1, 2\}  (F) none of these

Solution.  C.

(6) Which of the following is NOT a reduced residue system modulo 5?

(A) \{1, 2, 3, 4\}  (B) \{11, 12, 13, 14\}  (C) \{2, 4, 8, 16\}

(D) \{4, 8, 12, 16\}  (E) \{3, 9, 27, 81\}  (F) \{1, 9, 17, 36\}.

Solution.  F.
1 Use the Chinese Remainder Theorem to solve the linear diophantine system

\[
\begin{align*}
3x &\equiv 2 \pmod{5} \\
4x &\equiv 5 \pmod{7} \\
5x &\equiv 7 \pmod{11}
\end{align*}
\]

**Solution.** Observe that

\[
\begin{align*}
c_1 &= 4, c_2 = 3, c_3 = -3 \\
n_1 &= 77, n_2 = 55, n_3 = 35 \\
\bar{n}_1 &= 3, \bar{n}_2 = -1, \bar{n}_3 = 6.
\end{align*}
\]

So the solution to the system, by the Chinese Remainder Theorem, can be written as

\[
x \equiv 4 \times 77 \times 3 + 3 \times 55 \times (-1) + (-3) \times 35 \times 6 \equiv 129 \pmod{385}.
\]

Here 385 = 5 \times 7 \times 11.
2 Find the prime factorization for $31!$.

Solution.

\[
\left\lfloor \frac{31}{2} \right\rfloor + \left\lfloor \frac{31}{4} \right\rfloor + \left\lfloor \frac{31}{8} \right\rfloor + \left\lfloor \frac{31}{16} \right\rfloor = 15 + 7 + 3 + 1 = 26
\]

\[
\left\lfloor \frac{31}{3} \right\rfloor + \left\lfloor \frac{31}{9} \right\rfloor + \left\lfloor \frac{31}{27} \right\rfloor = 10 + 3 + 1 = 14
\]

\[
\left\lfloor \frac{31}{5} \right\rfloor + \left\lfloor \frac{31}{25} \right\rfloor = 6 + 1 = 7
\]

\[
\left\lfloor \frac{31}{7} \right\rfloor = 4
\]

\[
\left\lfloor \frac{31}{11} \right\rfloor = 2
\]

\[
\left\lfloor \frac{31}{13} \right\rfloor = 2
\]

\[
\left\lfloor \frac{31}{17} \right\rfloor = 1
\]

\[
\left\lfloor \frac{31}{19} \right\rfloor = 1
\]

\[
\left\lfloor \frac{31}{23} \right\rfloor = 1
\]

\[
\left\lfloor \frac{31}{29} \right\rfloor = 1
\]

\[
\left\lfloor \frac{31}{31} \right\rfloor = 1.
\]

So

\[
31! = 2^{26} \times 3^{14} \times 5^7 \times 7^4 \times 11^2 \times 13^2 \times 17 \times 19 \times 23 \times 29 \times 31
\]

is the prime factorization for $31!$. 
Let $p = 5$ and $q = 11$. So $n = pq = 55$ and $\phi(n) = (p - 1)(q - 1) = 40$. Bob chooses his public exponent $e = 27$ which is coprime with 40. Then he publishes his public key $(55, 27)$ openly.

(a) Compute Bob’s private key.

*Solution.* We need to solve $27d \equiv 1 \pmod{40}$.

Clearly we may choose $d = 3$ (or one may see this by Euclid’s algorithm). So $(55, 3)$ is Bob’s private key.

(b) Suppose that Alice wants to send an integer 15 to Bob. Compute the cyphertext $c$ she will send in the open channel.

*Solution.*

$$c \equiv 15^{27} \equiv (15^2)^{13} \times 15 \equiv 5^{13} \times 15 \equiv (5^3)^4 \times 75 \equiv 15^4 \times 20 \equiv 5^2 \times 20 \equiv 5 \pmod{55}$$

So Alice will send out 5.

(c) After receiving the cyphertext $c$, check that Bob is able to recover the original integer 15 using his private key.

*Solution.* Bob will recover the original integer by computing

$$m \equiv c^d \equiv 5^3 \equiv 125 \equiv 15 \pmod{55}.$$
Use Euclid’s division algorithm to find the general solution of the linear Diophantine equation
\[ 6x + 11y = 3. \]

**Solution.** Euclid’s algorithm:

\[
\begin{align*}
11 &= 6 \times 1 + 5 \\
6 &= 5 \times 1 + 1 \\
\end{align*}
\]

Now we have \(1 = 6 - 5 = 6 - (11 - 6) = 6 \times 2 + 11 \times (-1)\). Therefore

\[
6 \times 6 + 11 \times (-3) = 3
\]

and we get a solution \(x_0 = 6, y_0 = -3\). By our theory the general solution can be written in the shape

\[
\begin{align*}
x &= 6 + 11t \\
y &= -3 - 6t
\end{align*}
\]
5 Solve the linear congruence equation

\[ 7x \equiv 5 \pmod{15}. \]

**Solution.** We observe that \( 7 \times 13 \equiv 1 \pmod{15} \). So we multiply by 13 on both sides of the congruence and get

\[ 13 \times 7x \equiv 13 \times 5 \pmod{15}. \]

This is

\[ x \equiv 5 \pmod{15}. \]

So the set of solutions to the congruence are those integers which are congruent to 5 modulo 15.