CS:2210 Handwritten Homework 6

Section 4.1

#28. Decide whether each of these integers is congruent to 3 modulo 7.

a) 37

∴ Because $37 - 3 = 34$ is not divisible by 7, we see that $\boxed{37 \not\equiv 3 \pmod 7}$

∴ $\boxed{\text{No.}}$

b) 66.

∴ Because $66 - 3 = 63$ is divisible by 7, we see that $\boxed{66 \equiv 3 \pmod 7}$

∴ $\boxed{\text{Yes.}}$

#34. Show that if $a \equiv b \pmod m$ and $c \equiv d \pmod m$ where a, b, c, d and m are integers with $m \geq 2$, then $a - c \equiv b - d \pmod m$

∴ Use direct proof.

Because $a \equiv b \pmod m$ and $c \equiv d \pmod m$, by Theorem 4.

There are integers s and t with $b = a + sm$ and $d = c + tm$.

Hence, Using Subtract Equation,

If $b + d = (a+sm) + (c+tm)$
$= (a+c) + m(s+t)$.

then, $b - d = (a+sm) - (c+tm)$
$= (a-c) + m(s+t)$.

∴ Therefore, $(a-c) \pmod m = (b-d) \pmod m$

$(a-c) \equiv (b-d) \pmod m$

Section 4.2

#4. Convert the binary expansion of each of these integer to decimal expan.

a) $(1\ 1011)_2$

$1\times2^4 + 1\times2^3 + 1\times2 + 1$

$= 16 + 8 + 2 + 1$

$= \boxed{27}$

b) $(10\ 1011\ 0101)_2$

∴ $1\times2^9 + 1\times2^7 + 1\times2^5 + 1\times2^4 + 1\times2^2 + 1$

$= 512 + 128 + 32 + 16 + 4 + 1$

$= \boxed{693}$

c) $(11\ 1011\ 1110)_2$

∴ $1\times2^9 + 1\times2^8 + 1\times2^7 + 1\times2^5 + 1\times2^4 + 1\times2^3$
$+ 1\times2^2 + 1\times2$

$= 512 + 256 + 128 + 32 + 16 + 8 + 4 + 2$

$= \boxed{958}$

d) $(1111\ 1000\ 0011\ 111)_2$.

∴ $1\times2^{14} + 1\times2^{13} + 1\times2^{12} + 1\times2^{11} + 1\times2^{10} + 1\times2^4$
$+ 1\times2^3 + 1\times2^2 + 1\times2 + 1$

$= 16384 + 8192 + 4096 + 2048 + 1024 + 16$
$+ 8 + 4 + 2 + 1$

$= \boxed{31775}$

#12. Convert $(1\ 1000\ 0110\ 0011)_2$ to hexa. expansion.

∴ $(0001)_2\ (1000)_2\ (0110)_2\ (0011)_2$

$\downarrow\quad\downarrow\quad\downarrow\quad\downarrow$

$1\quad 8\quad 6\quad 3$

∴ $\boxed{(1863)_{16}}$

Section 4.3

#24

a) $2^2 \cdot 3^3 \cdot 5^5,\ 2^5 \cdot 3^3 \cdot 5^2$

$\therefore \gcd(2^2 \cdot 3^3 \cdot 5^5, 2^5 \cdot 3^3 \cdot 5^2)$

$= 2^{\min(2,5)} 3^{\min(3,3)} 5^{\min(5,2)}$

$= \boxed{2^2 \cdot 3^3 \cdot 5^2}$ $\therefore 56$

b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13,\ 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

$\therefore \gcd(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14})$

$= 2^{\min(1,11)} 3^{\min(1,9)} \cdot 11^{\min(1,1)}$

$= \boxed{2^1 \cdot 3^1 \cdot 11}$ $\therefore 66$

c) $17, 17^{17}$

$\therefore \gcd(17, 17^{17})$

$= 17^{\min(1,17)} = \boxed{17^1}$ $\therefore 17.$

#32. Use Euclidean Algorithm

a) $\gcd(1,5)$

$\therefore 5 = 1 \times 5$

Since 1 is the last nonzero remainder

$\gcd(1,5) = \boxed{1}$

b) $\gcd(100, 101)$

$\therefore 101 = 100 \times 1 + 1$

$100 = 1 \times 100.$

Since 1 is the last nonzero remainder

$\gcd(100,101) = \boxed{1}$

c) $\gcd(123, 277)$

$\therefore 277 = 123 \times 2 + 31$

$123 = 31 \times 3 + 30$

$31 = 30 \times 1 + 1$

$30 = 1 \times 30.$

Since 1 is the last nonzero remainder

$\gcd(123, 277) = \boxed{1}$

Section 4.4

#12 Ⓐ find inverses using Mathematica

→ see behind*

a) $34x \equiv 77 \pmod{89}$

$\therefore$ {g Bezout, {s Bezout, t Bezout}}

= Extended GCD[34, 89]

$\therefore$ output: {1, {-34, 13}}

Thus Bezout coefficients are -34 and 13.

Since $\boxed{-34}$ is negative, next positive number is 55. $\boxed{\text{Invers is 55}}$

b) $144x = 4 \pmod{233}$

$\therefore$ Input: {g Bezout, {s Bezout, t Bezout}}

= Extended GCD[144, 233]

Output: {1, [89, -55]}

Finding Bezout Coefficients,

$1 = 144 \times 89 - 233 \times 55$

$\boxed{\text{Inverse is 89.}}$

c) $200x = 13 \pmod{1001}$

$\therefore$ Input: {g Bezout, {s Bezout, t Bezout}} =

Extended GCD[200, 1001].

$\therefore$ Output: {1, {-5, 1}}

Finding Bezout coefficients.

$1 = 1001 \times 1 - 200 \times 5$

Inverse is $\boxed{-5}$, but since it is negative, next positive number is 966.

So $\boxed{\text{Inverse is 966.}}$

$\therefore$ Please see next page for #12.

#34. Use Fermat's little theorem to find 23^{1002} mod 41

∴ Fermat's little Theorem

⇒ If p is prime and a is an int. not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for every int. a we have

$$a^{p} \equiv a \pmod{p}.$$

∴ $a^{p-1} \equiv (1 \bmod p)$

⇒ $23^{40} \equiv 1 \pmod{41}$, $1001/40 = 25+3$

∴ $23^{1002} \pmod{41}$ =

$= (23^{40})^{25} \cdot 23^{2}$

$\equiv (1)^{25} \cdot 529 \pmod{41}$

$\equiv \boxed{37 \pmod{41}}$

∴ since $\frac{52}{41} = 12 \cdots 37$

#12 (B).

a) $34x \equiv 77 \pmod{89}$

∴ Inverse : 55

⇒ $34x \cdot 55 = 55 \cdot 77 \pmod{89}$

$1870 = 1 \pmod{89}$

$4235 = 52 \pmod{89}$

$x = 4235 \pmod{89}$

$\boxed{∴ x = 52 \pmod{89}}$

b) $144x = 4 \pmod{233}$

∴ Inverse : 89.

⇒ $144x \cdot 89 = 89 \cdot 4 \pmod{233}$

⇒ $12816 = 1 \pmod{233}$

$356 = 123 \pmod{233}$

∴ $x \equiv 356 \equiv 123 \pmod{233}$

$\boxed{∴ x = 123 \pmod{233}}$

c) $200x = 13 \pmod{1001}$

∴ Inverse : 966

$200x \cdot 966 = 966 \cdot 13 \pmod{1001}$

$199200 = 1 \pmod{1001}$

$12948 = 936 \pmod{1001}$

$\boxed{∴ x = 936 \pmod{1001}}$