Classroom Assignments of Lecture 4.

Section 1: 5 (a, b, c, d)

Section 2: 12 (e, g), 17.

Section 3: 1, 17 (a, b)

Section 4: 3, 7 (a), 9 (a, b, c, d), 22 (b)

Section 5: 18 (a, c).

Review Section of Chapter 11, 26, 27.

Section 1.

5 Find the quotient q and r.

(a) $a = 5286$, $b = 19$.

$a > 0$, $b > 0$. $a = bq + r$, $0 \le r < b$.

$$q = \left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{5286}{19} \right\rfloor = 278.$$

$$r = a - bq = 5286 - 278 \cdot 19 = 4.$$

$$\Rightarrow \boxed{5286 = 19 \cdot 278 + 4.} \quad //$$

(b) $a = -5286$, $b = 19$.

$a < 0$. Take $-a = 5286$.

$-a = bq + r \Rightarrow a = b(-q) - r =$

$= (-q-1)b + (b-r)$ if > 0.

$-5286 = 19(-278) - 4 =$

$= 19(-278-1) + (19-4) = 19 \cdot (-279) + 15$

$$\boxed{-5286 = 19 \cdot (-279) + 15} \quad //$$

(c) $a = 5286$, $b = -19$.

Take $-b = 19$.

$a = (-b)q + r = b(-q) + r$.

$5286 = (-b)q + r = (-19) \cdot (-278) + 4$

$$\boxed{5286 = (-19) \cdot (-278) + 4.,} \quad 0 \le 4 \le |-19|. \; //$$

(d.) $a = -5286$, $b = -19$.

$-a = 5286 > 0$ and $-b = 19 > 0$.

$-a = (-b)q + r$. $\quad a = bq - r = (-b)(-q) - r =$

$= (-b)(-q-1) + (b-r)$

$5286 = 19 \cdot 278 + 4 \Rightarrow -5286 = (-19)\cdot 278 - 4$

$= 19(-278) - 4 =$

$= 19(-278-1) + (19-4)$

$= 19 \cdot (-279) + 15.$

$= (-19)(279) + 15.$

So $\boxed{-5286 = (-19)\cdot 279 + 15.}$ //

Section 2

12. Find GCD of a and b and express it in the form ma + nb for suitable integers m and n.

(e). $a = 1575$, $b = -231$.

Solution

$1575 = (231)\cdot(-6) + 189$

$-231 = 189\cdot(-1) - 42 = 189(-2) + 147$

$189 = 147\cdot 1 + 42$

$147 = 42\cdot 3 + 21$

$42 = 21\cdot 2 + 0$.

The nonzero last remainder is 21.

Hence $GCD(1575, -231) = 21$.

$21 = 147 - 42\cdot 3 = 147 - (189 - 147)\cdot 3 =$

$= 147 - 189\cdot 3 + 147\cdot 3 = 147\cdot 4 - 189\cdot 3 =$

$= [-231 - 189\cdot(-2)]\cdot 4 - 189\cdot 3 =$

$= -231\cdot 4 + 189\cdot 8 - 189\cdot 3 =$

$= -231\cdot 4 + 189\cdot 5 = -231\cdot 4 + [1575 - (-231)\cdot(-6)]\cdot 5$

$= -231\cdot 4 + 1575\cdot 5 + (-231)\cdot 30 =$

$= -231\cdot 34 + 1575\cdot 5$

So $\boxed{21 = 34(-231) + 5\cdot 1575}$ //

9). Solution

$a = -3719$. $b = 8416$.

$-3719 = 8416 \cdot 0 - 3719 = 8416 \cdot (-1) + 4697$

$8416 = 4697 \cdot 1 + 3719$

$4697 = 1 \cdot 3719 + 978$

$3719 = 3 \cdot 978 + 785$

$978 = 1 \cdot 785 + 193$

$785 = 4 \cdot 193 + 13$

$193 = 14 \cdot 13 + 11$

$13 = 1 \cdot 11 + 2$

$11 = 5 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$.

The nonzero last remainder is 1.

So $GCD(-3719, 8416) = 1$.

$1 = 11 - 5 \cdot 2 = 11 - 5 \cdot (13 - 11) = 11 - 5 \cdot 13 +$

$+ 5 \cdot 11 = 6 \cdot 11 - 5 \cdot 13 = 6 \cdot (193 - 14 \cdot 13) - 5 \cdot 13 =$

$= 6 \cdot 193 - 84 \cdot 13 - 5 \cdot 13 = 6 \cdot 193 - 89 \cdot 13 =$

$= 6 \cdot 193 - 89 \cdot (785 - 4 \cdot 193) =$

$= 6 \cdot 193 - 89 \cdot 785 + 356 \cdot 193 = 362 \cdot 193 -$

$- 89 \cdot 785 = 362 \cdot (978 - 785) - 89 \cdot 785 =$

$= 362 \cdot 978 - 362 \cdot 785 - 89 \cdot 785 =$

$= 362 \cdot 978 - 451 \cdot 785 =$

$= 362 \cdot 978 - 451 \cdot (3719 - 3 \cdot 978) =$

$= 362 \cdot 978 - 451 \cdot 3719 + 1353 \cdot 978 =$

$= 1715 \cdot 978 - 451 \cdot 3719 =$

$= 1715 \cdot (4697 - 3719) \cdot - 451 \cdot 3719 =$

$= 1715 \cdot 4697 - 1715 \cdot 3719 - 451 \cdot 3719 =$

$= 1715 \cdot 4697 - 2166 \cdot 3719 =$

$= 1715 \cdot 4697 - 2166 \cdot (8416 - 4697) =$

$= 1715 \cdot 4697 - 2166 \cdot 8416 + 2166 \cdot 4697 =$

$= 3881 \cdot 4697 - 2166 \cdot 8416 =$

$= 3881 (-3719 + 8416) - 2166 \cdot 8416 =$

$= 3881 \cdot (-3719) + 3881 \cdot 8416 - 2166 \cdot 8416 =$

$= 3881 \cdot (-3719) + 1715 \cdot 8416$

$\Rightarrow \boxed{1 = 3881 \cdot (-3719) + 1715 \cdot 8416.}$ //

17.

(a) $17369x + 5472y = 4.$

Solution:

$17369 = 5472 \cdot 3 + 953$

$5472 = 953 \cdot 5 + 707$

$953 = 707 \cdot 1 + 246$

$707 = 246 \cdot 2 + 215$

$246 = 215 \cdot 1 + 31$

$215 = 31 \cdot 6 + 29$

$31 = 29 \cdot 1 + 2$

$29 = 2 \cdot 14 + 1$

$14 = 1 \cdot 14 + 0$

$\Rightarrow GCD(17369, 5472) = 1.$

$17369x + 5472y = 4$ has a solution.

$1 = 29 - 2 \cdot 14 = 29 - (31 - 29) \cdot 14 = 29 - 31 \cdot 14 + 29 \cdot 14$

$= 29 \cdot 15 - 31 \cdot 14 = (215 - 31 \cdot 6) 15 - 31 \cdot 14 =$

$= 215 \cdot 15 - 31 \cdot 90 - 31 \cdot 14 = 215 \cdot 15 - 31 \cdot 104 =$

$= 215 \cdot 15 - (246 - 215) \cdot 104 = 215 \cdot 15 - 246 \cdot 104$

$+ 215 \cdot 104 = 215 \cdot 119 - 246 \cdot 104 = (707 - 246 \cdot 2) \cdot 119$

$- 246 \cdot 104 = 707 \cdot 119 - 246 \cdot 238 - 246 \cdot 104$

$= 707 \cdot 119 - 246 \cdot 342 = 707 \cdot 119 - (953 - 707) \cdot 342$

$= 707 \cdot 119 - 953 \cdot 342 + 707 \cdot 342 =$ 461

$= 707 \cdot 461 - 953 \cdot 342 = (5472 - 953 \cdot 5) \cdot$

$- 953 \cdot 342 = 5472 \cdot 461 - 953 \cdot 2305 - 953 \cdot 342 =$

$= 5472 \cdot 461 - 953 \cdot 2647 = 5472 \cdot 461 -$

$(17369 - 5472 \cdot 3) \cdot 2647 =$

$= 5472 \cdot 461 - 17369 \cdot 2647 + 5472 \cdot 7941$

$= 5472 \cdot 8402 - 17369 \cdot 2647$

Sо $\quad 1 = 5472 \cdot 8402 - 17369 \cdot 2647$

$4 \cdot 1 = 5472 \cdot (4 \cdot 8402) - 17369 \cdot (4 \cdot 2647)$

$4 = 5472y + 17369y$

$\Rightarrow y_0 = 4 \cdot 8402 = 33608$

$x_0 = -4 \cdot 2647 = -10588.$

$x = -10588 + 5472t \quad t := t+2 \Rightarrow$

$y = 33608 - 17369t$

$$\boxed{\begin{aligned} x &= 356 + 5472t \\ y &= -1130 - 17369t \end{aligned}} \quad \text{ang } t \in \mathbb{Z}$$

//

(b). $154x + 260y = 4$.

Solution.

$154 = 260 \cdot 0 + 154$

$260 = 154 \cdot 1 + 106$

$154 = 106 \cdot 1 + 48$

$106 = 48 \cdot 2 + 10$

$48 = 10 \cdot 4 + 8$

$10 = 8 \cdot 1 + 2$

$8 = 2 \cdot 4 + 0$

GCD $(154, 260) = 2$ and divides 4.

the Diophantine equation has a solution.

$2 = 10 - 8 = 10 - (48 - 10 \cdot 4) = 5 \cdot 10 - 48 =$

$= 5 \cdot (106 - 2 \cdot 48) - 48 = 5 \cdot 106 - 11 \cdot 48 =$

$= 5 \cdot 106 - 11 (154 - 106) = 16 \cdot 106 - 11 \cdot 154 =$

$= 16 (260 - 154) - 11 \cdot 154 = 16 \cdot 260 - 27 \cdot 154$

$2 = 16 \cdot 260 - 27 \cdot 154$

$4 = 32 \cdot 260 - 54 \cdot 154.$

$x_0 = -54, \quad y_0 = 32.$

$$\boxed{\begin{aligned} x &= -54 + 130t \\ y &= 32 - 77t \end{aligned}} \qquad t \in \mathbb{Z}. \quad //$$

(c) $154x + 260y = 3$

GCD(154, 260) = 2 and 2 does not divide 3. Then $154x + 260y = 3$ has no integer solutions.

Section 3

1. Determine whether each of the following integers is a prime.

(a) 157

$\sqrt{157} \approx 12.53$

$1 < 2, 3, 5, 7, 11 < 12$

2, 3, 5, 7 and 11 do not divide and therefore 157 is prime.

(b) 9831

Since $9+8+3+1$ is divisible by 3
9831 is divisible by 3.
Hence 9831 is not divisible by 3.

(c) 9833

$\sqrt{9833} \approx 99$

Any prime number n $(2 \leq n < 99)$ does not divide 9833. Then 9833 is prime.

(d) 55551111

Since $5+5+5+5+1+1+1+1 = 24$
and it is divisible by 3, hence
55551111 is divisible by 3.

So 55551111 is not prime.

(e). $2^{216000} - 1 = 2^{2 \cdot 108000} - 1 =$

$= (2^{108000} - 1)(2^{108000} + 1)$.

So $2^{216000} - 1$ is not prime.

17. (a, b).

$n \in \mathbb{N}$. $d(n) :=$ the number of positive divisors of n.

(a) $d(n) = 2$. Then n is prime. Since only prime numbers have 2 divisors //

(b). $d(n) = 3$

$n = p^2 \Rightarrow$ $d(n) = 3$ since $1, p, p^2$ are divisors of n.

If n has two distinct divisors say p and q, then $d(n) \geq 4$

Since $1, p, q, pq$ are divisors of n.

Therefore $n = p^2$ //

Section 4

3. Find $a \pmod n$

(a) $a = 1286, \quad n = 39.$

$1286 = 39 \cdot 32 + 38$

$1286 \pmod{39} \equiv 38$

(b) $a = 43197, \quad n = 333.$

$43197 = 333 \cdot 129 + 240.$

$43197 \pmod{333} \equiv 240.$

(c). $a = -545608, \quad n = 51.$

$-545608 = 51 \cdot (-10698) - 10 =$

$= 51(-10699) + 41$

Then

$-545608 \pmod{51} \equiv 41.$

(d) $a = -125617, \quad n = 315$

$-125617 = 315(-398) - 247. =$

$= 315(-399) + 68$

Then $-125617 \pmod{315} \equiv 68.$

(e) $a = 11\,111\,111\,111 \quad n = 1111$

$11\,111\,111\,111 = 1111 \cdot 10\,000\,000 + 111$

Then $11\,111\,111\,111 \pmod{1111} \equiv 111$. //

7(a). $a = 4003$, $b = -127$, $n = 85$

Find $a+b \pmod n$, $ab \pmod n$, $(a+b)^2 \pmod n$

Solution: $a+b = 4003 - 127 = 3876$.

$3876 = 85 \cdot 45 + 51$.

$3876 \pmod{85} \equiv \underline{51}$.

$a \cdot b = 4003 \cdot (-127) = -508381 =$

$= 85(-5980) - 81 = 85(-5981) + 4$

Then $4003 \cdot (-127) \pmod{85} \equiv \underline{4}$.

$(a+b)^2 \bmod n \equiv (51)^2 \pmod{85} =$

$= 2601 \pmod{85} \equiv \underline{51}$

Since $2601 = 85 \cdot 30 + 51$. //

$g(a, b, c, d)$.

(a) $3x \equiv 4 \pmod 6$

$x \in \{0, 1, 2, 3, 4, 5\}$.

$3 \cdot 0 \equiv 0 \pmod 6$
$3 \cdot 1 \equiv 3 \pmod 6$
$3 \cdot 2 \equiv 0 \pmod 6$
$3 \cdot 3 \equiv 3 \pmod 6$
$3 \cdot 4 \equiv 0 \pmod 6$
$3 \cdot 5 \equiv 3 \pmod 6$

$\Rightarrow 3x \equiv 4 \pmod 6$ has no solution.

(b) $4x \equiv 2 \pmod 6$

$x \in \{0, 1, \ldots, 5\}$

$4 \cdot 0 \equiv 0 \pmod 6$
$4 \cdot 1 \equiv 4 \pmod 6$
$4 \cdot 2 \equiv 2 \pmod 6$
$4 \cdot 3 \equiv 0 \pmod 6$
$4 \cdot 4 \equiv 4 \pmod 6$
$4 \cdot 5 \equiv 2 \pmod 6$

$x = 2, 5$ are solutions of $4x \equiv 2 \pmod 6$.

(c). $4x \equiv 3 \pmod 7$.

$4 \cdot 0 \equiv 0 \pmod 7$
$4 \cdot 1 \equiv 4 \pmod 7$
$4 \cdot 2 \equiv 1 \pmod 7$
$4 \cdot 3 \equiv 5 \pmod 7$
$4 \cdot 4 \equiv 2 \pmod 7$
$4 \cdot 5 \equiv 6 \pmod 7$
$4 \cdot 6 \equiv 3 \pmod 7$

$x = 6$

(d). $4x \equiv 3 \pmod 6$

$x \in \{0, 1, \ldots, 5\}$

$4 \cdot 0 \equiv 0 \pmod 6$

$4 \cdot 1 \equiv 4 \pmod 6$

$4 \cdot 2 \equiv 2 \pmod 6$

$4 \cdot 3 \equiv 0 \pmod 6$

$4 \cdot 4 \equiv 4 \pmod 6$

$4 \cdot 5 \equiv 2 \pmod 6$

} no solution. //

22. (b)

$53^{20592} \equiv ? \pmod{20593}$

By the Fermat's Little theorem

if $GCD(a, p) = 1$ and

then $a^{p-1} \equiv 1 \bmod p$.

Since 20593 is prime and

$GCD(53, 20593) = 1$

we have $53^{20592} \equiv 1 \pmod{20593}$.

$$53^{20593} = 53 \cdot 53^{20592} \equiv 53 \cdot 1 \pmod{20593}$$

$$53^{20594} = 53^2 \cdot 53^{20592} \equiv 53^2 \cdot 1 \pmod{20593}$$

$$= 2809 \pmod{20593} \quad //$$

Section 5

18. (a) $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$

$N = 35.$

$x = \frac{35}{5} 3 \cdot b_1 + \frac{35}{7} 4 \cdot b_2 \pmod{35}$

$= 21 b_1 + 20 b_2 \pmod{35}.$ ☺

$7 b_1 \equiv 1 \pmod 5$ $\qquad$ $5 b_2 \equiv 1 \pmod 7$

$2 b_1 \equiv 1 \pmod 5$ $\qquad$ $b_2 \equiv 3 \pmod 7$

$b_1 \equiv 3 \pmod 5$

$= 21 \cdot 3 + 20 \cdot 3 = 63 + 60 = 123 \pmod{35}$

$\equiv 18 \pmod{35}$

$\boxed{x \equiv 18 \pmod{35}}$ //

(c) $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 7 \pmod 8 \end{cases}$

$N = 40$

$x = \frac{40}{5} \cdot 3 \cdot b_1 + \frac{40}{8} \cdot 7 b_2 \pmod{40} =$

$= 24 b_1 + 35 b_2 \pmod{40} = (24 \cdot 2 + 35 \cdot 5) \pmod{40}$

$8 b_1 \equiv 1 \pmod 5$

$3 b_1 \equiv 1 \pmod 5$

$b_1 \equiv 2 \pmod 5$

$5 b_2 \equiv 1 \pmod 8$

$b_2 \equiv 5 \pmod 8$

$= 223 \pmod{40}$

$= 23 \pmod{40}$

$\boxed{x \equiv 23 \pmod{40}}$ //