Kenneth Jahnke

Assignment 2 – 25 Jan 2025

CSCI 389 (Online) - Spring ‘25

2.1.

Reforumlation:

Given any positive integer n and any integer a, if we divide a by n, we get an integer quotient q and an integer remainder r that obey the following relationship:

$a = qn + r$ where $0 \leq r < n$; $q = \lfloor a / n \rfloor$

There is no requirement for a to be non-negative. (I don’t know why the textbook version of this equation says so, especially given they used a negative integer a in an example.) For this reformulation that specifically requests the removal of restrictions on a to work, all that’s required is for n to be positive.

Examples:

$a = -33$; $n = 9 \therefore q = \lfloor -33 / 9 \rfloor = -4$

$-33 = -4 (9) + r$

$-33 = -36 + r$

$-33 + 36 = r$

$3 = r$

$a = -11$; $n = 7 \therefore q = \lfloor -11 / 7 \rfloor = -2$

$-11 = -2 (7) + r$

$-11 = -14 + r$

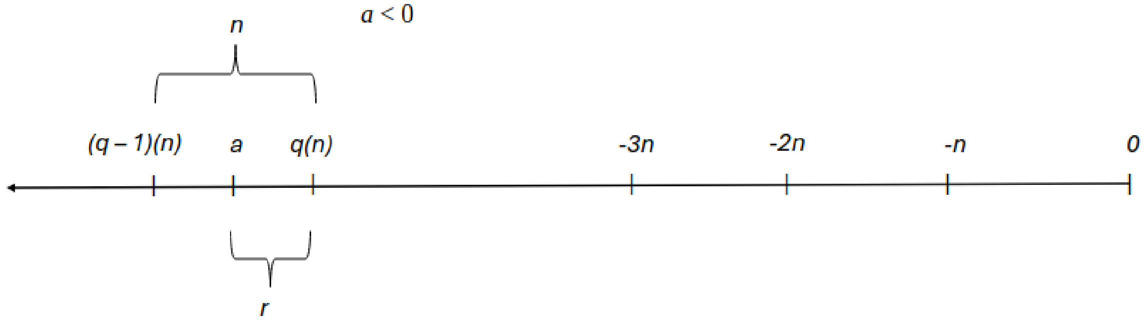
$-11 + 14 = r$

$3 = r$

2.2.

$a = qn + r$ where $0 \leq r < n$; $q = \lfloor a / n \rfloor$

$a < 0$



2.3.a.

$4 \equiv 1 \pmod{3}$

$5 \equiv 2 \pmod{3}$ [Note: x]

$2x \equiv 1 \pmod{3}$

$2 \bullet 2 = 4$ and $4 \equiv 1 \pmod{3}$ $\therefore$ $x = 2$

x = 2

2.3.b.

$6 \equiv 1 \pmod{5}$

$7 \equiv 2 \pmod{5}$ [Note: x]

$2x \equiv 1 \pmod{5}$

$2 \bullet 3 = 6$ and $6 \equiv 1 \pmod{5}$ $\therefore$ $x = 3$

x = 3

2.3.c.

$8 \equiv 1 \pmod{7}$

$9 \equiv 2 \pmod{7}$ [Note: x]

$2x \equiv 1 \pmod{7}$

$2 \bullet 4 = 8$ and $8 \equiv 1 \pmod{7}$ $\therefore$ $x = 4$

x = 4

2.4.a

5 mod 3 = 2

$\lfloor 5 / 3 \rfloor = 1 = q$

5 = 1(3) + r

r = 2

2.4.b.

5 mod –3 = -1

$\lfloor 5 / -3 \rfloor = -2 = q$

5 = -2(-3) + r

r = -1

2.4.c.

-5 mod 3 = 1

$\lfloor 5 / -3 \rfloor = -2 = q$

-5 = -2(3) + r

r = 1

2.4.d.

-5 mod -3 = -2

$\lfloor -5 / -3 \rfloor = 1 = q$

-5 = 1(-3) + r

r = -2

2.7.

k = 1

Smallest: 1

Divisors: 1

k = 2

Smallest: 2

Divisors: 1, 2

k = 3

Smallest: 4

Divisors: 1, 2, 4

k = 4

Smallest: 6

Divisors: 1, 2, 3, 6

k = 5

Smallest: 16

Divisors: 1, 2, 4, 8, 16

k = 6

Smallest: 12

Divisors: 1, 2, 3, 4, 6, 12

2.10.

$1x \equiv 1 \pmod{5} \rightarrow x = 1$

$2x \equiv 1 \pmod{5} \rightarrow x = 3$

$3x \equiv 1 \pmod{5} \rightarrow x = 2$

$4x \equiv 1 \pmod{5} \rightarrow x = 4$

2.11.

321 mod 9 = 6

$321 = 35(9) + 6$

$3 + 2 + 1 = 6$

6 mod 9

$6 = 0(9) + 6$

$321 \equiv 3 + 2 + 1 \equiv 6 \pmod{9}$

2.12.a.

$24140 = 1 \cdot 16762 + 7378$

$16762 = 2 \cdot 7378 + 2006$

$7378 = 3 \cdot 2006 + 1360$

$2006 = 1 \cdot 1360 + 646$

$1360 = 2 \cdot 646 + 68$

$646 = 9 \cdot 68 + 34$

$68 = 2 \cdot 34 + 0$

$\gcd(24140, 16762) = 34$

2.12.b.

$12075 = 2 \cdot 4655 + 2765$

$4655 = 1 \cdot 2765 + 1890$

$2765 = 1 \cdot 1890 + 875$

$1890 = 2 \cdot 875 + 140$

$875 = 6 \cdot 140 + 35$

$140 = 4 \cdot 35 + 0$

$\gcd(4655, 12075) = 35$

2.16.a.

4321 = 3 • 1234 + 619

1234 = 1 • 619 + 615

619 = 1 • 615 + 4

615 = 153 • 4 + 3

4 = 1 • 3 + 1

3 = 3 • 1 + 0

gcd = 1

q	r1	r2	r	s1	s2	s	t1	t2	t
3	4321	1234	619	1	0	1	0	1	-3
1	1234	619	4	0	1	-1	1	-3	4
153	619	4	3	1	-1	154	-3	4	-615
1	4	3	1	-1	154	-155	4	-615	619
3	3	1	0	154	-155	619	-615	619	-2472
	1	0		-155	619		619	-2472	

Multiplicative inverse: 619

2.16.b.

40902 = 1 • 24140 + 16762

24140 = 1 • 16762 + 7378

16762 = 2 • 7378 + 2006

7378 = 3 • 2006 + 1360

2006 = 1 • 1360 + 646

1360 = 2 • 646 + 68

646 = 9 • 68 + 34

68 = 2 • 34 + 0

gcd = 34

No multiplicative inverse.

2.16.a.

1769 = 3 • 550 + 119

550 = 4 • 119 + 74

119 = 1 • 74 + 45

74 = 1 • 45 + 29

45 = 1 • 29 + 16

29 = 1 • 16 + 13

16 = 1 • 13 + 3

13 = 4 • 3 + 1

3 = 3 • 1 + 0

gcd = 1

q	r1	r2	r	s1	s2	s	t1	t2	t
3	1769	550	119	1	0	1	0	1	-3
4	550	119	74	0	1	-4	1	-3	13
1	119	74	45	1	-4	5	-3	13	-16
1	74	45	29	-4	5	-9	13	-16	29
1	45	29	16	5	-9	14	-16	29	-45
1	29	16	13	-9	14	-23	29	-45	74
1	16	13	3	14	-23	37	-45	74	-119
4	13	3	1	-23	37	-171	74	-119	550
3	3	1	0	37	-171	550	-119	550	1769
	1	0		-171	550		550	1769	

Multiplicative inverse: 550

2.19. If d is the common divisor of n and $n + 1$ then we can say,

$d \mid n$; $d \mid (n + 1)$

$d \mid ((n + 1) - 1)$, or $d \mid 1$

1 is the integer that divides itself, therefore $d = 1$. 1 divides any number larger than it, hence the greatest common factor of 1 and any other integer is 1.