M366 Set 1

Problem 1) a) Find quotient and remainder

$108 = 3m + r$ $\quad m = 36$ $\quad r = 0$

quotient remainder

b) $129 = 7m + r$ $\quad 140_{20} - 14_2 = 126$ $\quad m = 18$ $\quad r = 3$

c) $\ldots 2 + \ldots 1 = \ldots 3 \equiv 3 \bmod 5$

d) Friday $= 0$ $\quad 779 \bmod 7 = 2$ $\quad m = 111$ $\quad r = 2$

Problem 2) a) $(81 * 13) \bmod 10 \equiv 1 * 3 \bmod 10 \equiv 3$

b) $(14 + 3 * 26) \bmod 3 \equiv 2 + 0(2) \bmod 3 \equiv 2$

c) $(17 + x) \equiv 0 \bmod 4$ $\quad 1 + x \equiv 0 \bmod 4$ $\quad x \equiv 3 \bmod 4$

d) given $x \equiv 5 \bmod 8$, $y \equiv 6 \bmod 8$ find $x+y$ & xy mod 8

$x+y \rightarrow 5+6 = 11 \bmod 8 \equiv 3$

$xy \rightarrow 5 \cdot 6 = 30 \bmod 8 \equiv 6$

Problem 3) a) $3^{100} \bmod 11 \equiv (3^{10})^{10} \bmod 11 \equiv 1^{10} \bmod 11 \equiv 1$

Euler's Thrm: $a^{p-1} \equiv 1 \bmod p$

b) $5^{12345} \bmod 12 \equiv 5$

look for a pattern in the powers $\rightarrow 5^1 \equiv 5$; $5^2 \equiv 1$; $5^3 \equiv 5$; $5^4 \equiv 1$

Problem 4) $n \geq 0, n \in \mathbb{Z}$ $\quad (3^{2n+1} + 2^{n+2}) \equiv 0 \bmod 7$ $\quad$ show

$(3^2)^n \cdot 3 + 2^n \cdot 2^2 \rightarrow 9^n \cdot 3 + 2^n \cdot 4 \pmod 7 \rightarrow 2^n \cdot 3 + 2^n \cdot 4$

$9 \equiv 2$

$\rightarrow 2^n(3+4) \bmod 7 \rightarrow 2^n(0) \bmod 7 \equiv 0$

Problem 5) a) $\phi(7) = 7(1-\frac{1}{7}) = 7(\frac{6}{7}) = 6$

b) $\phi(49) = 49(1-\frac{1}{7}) = 49\frac{6}{7} = 7 \cdot 6 = 42$

c) $\phi(35) = 35(1-\frac{1}{7})(1-\frac{1}{5}) = 35 \cdot \frac{6}{7} \cdot \frac{4}{5} = 24$

d) $\phi(100) = 100(1-\frac{1}{2})(1-\frac{1}{5}) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$

M366 Set 2

Problem 1) 3^{162} mod 17 $\rightarrow (3^{10})^{16} \cdot 3^2 \equiv 1 \cdot 3^2 \equiv 9$

Problem 2) $n \in \mathbb{Z}, n \geq 0$ show $(2 * 4^{3n+1} + 5^{2n+1}) \equiv 0 \mod 13$

$2 \cdot 64^n \cdot 4 + 25^n \cdot 5 \rightarrow 8 \cdot 12^n + 12^n \cdot 5 \rightarrow 12^n(8+5) \mod 13$

$\rightarrow 12^n(0) \equiv 0 \mod 13$

Problem 3) $\phi(7^3 \cdot 5^2) = 7^3 \cdot 5^2 (\frac{6}{7})(\frac{4}{5}) = 7^2 \cdot 5 \cdot 24 = 49 \cdot 120$

b) let $n = 7^3 * 5^2 * 11^5$ find $\phi(n)$ $\quad \phi(n) = n(\frac{6}{7} \cdot \frac{4}{5} \cdot \frac{10}{11})$

$= 7^2 \cdot 5 \cdot 11^4 \cdot 240 = 1200 \cdot 7^2 \cdot 11^4$

c) $\phi(10000) = 10^4(\frac{1}{2} \cdot \frac{4}{5}) = 10^3 \cdot 4 = 4000$

$(10)^4$

Problem 4) a) show 100 and 31 are coprime

$\rightarrow \gcd(100, 31) = 1$

$100 = 31 \cdot 3 + 7$

$31 = 7 \cdot 4 + 3$

$7 = 3 \cdot 2 + 1$ ✓

$3 = 1 \cdot 3 + 0$

[redacted]

~~$4\times 8 = 32$ $\quad$ $4\times 8 = 32$~~

~~$18\times 12 = 96$ $\quad$ $12\times 10 = 120$ $\quad$ 27. c~~

~~128 $\quad$ 152 $\quad$ 28. c or a~~

b) find integer k s.t. $0 < k < 100$ s.t. $31k \equiv 1 \bmod 100$

$1 = 7 - 3\cdot 2$

$1 = 7 - (31 - 7\cdot 4)\cdot 2 = 7 - 2\cdot 31 + 2\cdot 7\cdot 4 = 7 - 2\cdot 31 + 8\cdot 7$

$1 = 9\cdot 7 - 2\cdot 31$

$1 = 9(100 - 31\cdot 3) - 2\cdot 31 = 9\cdot 100 - 27\cdot 31 - 2\cdot 31 = \underline{9}\cdot 100 - \underline{29}\cdot 31$

$-29 \bmod 100 = \underline{71}$ $\quad$ $k = 71$

c) $9\cdot 100 - 29\cdot 31 \bmod 31 \rightarrow 9\cdot 100 \bmod 31 = 9$

Problem 5) a) find the equivalence classes of integers that are units under multiplication mod 15

(find the integers 1 to 14 in which $\gcd(15, n) = 1$

$\varphi(15) = 15\left(\frac{2}{3}\cdot\frac{4}{5}\right) = 8$ is the size of the set

$\{1, 2, 4, 7, 8, 11, 13, 14\}$ ✓

b) multiplication table for the equivalence classes of integers that are units under multiplication mod 14

$\varphi(14) = 14\left(\frac{6}{7}\cdot\frac{1}{2}\right) = 6$ $\quad$ $\{1, 3, 5, 9, 11, 13\}$

	1	3	5	9	11	13
1	1	.	-	-	-	-
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

c) addition table mod 5

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

Problem 6) a) Unique identity element $\quad a\cdot e_1 = a \quad a\cdot e_2 = a \quad$ so $\quad e_1 e_2 = e_1$

$e_1\cdot a = a \quad e_2\cdot a = a \quad e_1\cdot e_2 = e_2$

b) $a, b, c \in G$ $\quad$ suppose b and c are inverses of a

$a\cdot b = e \quad a\cdot c = e \quad \cancel{a}\cdot b = \cancel{a}\cdot c \quad b = c$

or $b = be = b(a\cdot c) = (b\cdot a)\cdot c = ec = c$

c) $ac = b \rightarrow (a^{-1}a)c = ba^{-1} \rightarrow c = ba^{-1}$

The group is closed under the operation so if a^{-1} (which is unique) and b exist in G then c exists