HW Week 8

$a = dq + r$ $\quad q = \frac{a}{d}$

Problem 1: What are the quotient & remainder when

a) 19 is divided by 7? $\quad 2(5)$

b) -111 is divided by 11? $\quad -11(10)$

$a = -111$

$b = 11$

$-111 = 11 \cdot (-10) + r$

$r = -111 + 110 = -1$

$-111 = 11q + r$

$11 \times (-11) = -121$

$q = -11$, then.

$-111 = -121 + r$

$121 - 111 = r$

$r = 10$.

remainder is always positive, we go over to the next one.

c) 789 divided by 23? $\quad 34(7)$ ✓

d) 1001 is divided by 13? $\quad 77(0)$ ✓

e) 0 divided by 19 $\quad 0 \quad \times \quad 0(0)$

f) 3 divided by 5? $\quad \left|\frac{3}{5}\right| \quad \times$

$a = 3$

$d = 5$

$0 \leq r < d$

$0 \leq r < 5$

$3 = 5 \cdot 0 + 3 \Rightarrow$ so $q = 0$, $r = 3$.

g) -1 divided by 3? $\quad \left|\frac{1}{3}\right| \quad \times \quad -1 = 3 \cdot (-1) + 2$ $\quad q = -1$, $r = 2$.

h) 4 is divided by 1? $\quad 4(0)$

Problem 2 Find a formula for the integer with smallest absolute value that is congruent to an integer a modulo m, where m is a positive integer.

$a \bmod m = b \bmod m$.

Problem 3: Find counterexamples to each of these statements about congruences.

a) If $ac \equiv bc \pmod{m}$, where a, b, c, and m are integers with $m \geq 2$, then $a \equiv b \pmod{6}$.

$14 \equiv 8 \pmod{6}$. ✗

$7 \not\equiv 4 \pmod{6}$.

Solution Let $m = 4$. $c = 2$.

let $a = 0$ $b = 2$ $\Rightarrow$ $ac = 0$

$ac \equiv bc \pmod{4}$

but $0 \not\equiv 2 \pmod{4}$

b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d, and m are integers with c and d positive and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$

$14 \equiv 8 \pmod{6}$ $\quad$ $7 \equiv 1 \pmod{6}$

$14^1 \not\equiv 8^7$

Solution: $a^c \not\equiv b^d \pmod{m}$

Let $m = 5$ $\quad$ $b = 3$

$a = 3$ $\quad$ $c = 1$ $\quad$ $d = 6$.

$a^c \Rightarrow 3^1 \equiv 3^6$ $\quad$ $b^d = 729 = 4 \pmod{5}$.

do $3^1 \not\equiv 3^6 \pmod{5}$, even though $3 = 3 \pmod{5}$ and $1 = 6 \pmod{5}$

Problem 4: Show that if a, b, k and m are int-s such that $k \geq 1$ $m \geq 2$, and $a \equiv b \pmod m$ then $a^k \equiv b^k \pmod m$.

Problem 5: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4, \cancel{5}\}$

Add-n modulo

1) $a +_m b = (a+b) \bmod m$.

We add $(a+b)$ and then find the remainder when the result is divided by 5. This remainder will be the sum in $\mathbb{Z}_5$.

$/5=0$

$0+0=0$	$0+1=1$	$0+2=2$	$0+3=3$	$0+4=4$
$1+0=1$	$1+1=2$	$1+2=3$	$1+3=3$	$1+4=5/5=0$ mod
$2+0=2$	$2+1=3$	$2+2=4$	$2+3=5=0$	$2+4=6=1$
$3+0=3$	$3+1=4$	$3+2=5=0$	$3+3=1$	$3+4=2$
$4+0=4$	$4+1=0$	$4+2=6 \to 1$	$4+3=2$	$4+4=3$

$0 \cdot 0 = 0$	$0 \cdot 1 = 0$	$0 \cdot 2 = 0$	$0 \cdot 3 = 0$	$0 \cdot 4 = 0$
$1 \cdot 0 = 0$	$1 \cdot 1 = 1$	$1 \cdot 2 = 2$	$1 \cdot 3 = 3$	$1 \cdot 4 = 4$
$2 \cdot 0 = 0$	$2 \cdot 1 = 2$	$2 \cdot 2 = 4$	$2 \cdot 3 = 6 = 1$	$2 \cdot 4 = 3$
$3 \cdot 0 = 0$	$3 \cdot 1 = 3$	$3 \cdot 2 = 1$	$3 \cdot 3 = 4$	$3 \cdot 4 = 2$
$4 \cdot 0 = 0$	$4 \cdot 1 = 4$	$4 \cdot 2 = 3$	$4 \cdot 3 = 2$	$4 \cdot 4 = 1$

Problem 6: Determine whether each of the fns f $f(a) = a \text{ div } d$ and $g(a) = a \bmod d$, where d is a positive int from the set of int-s, is one-to-one, and determine whether each of these fns is onto.

1) $f(a) = a \text{ div } d$ → takes an int a as an input & returns the integer quotient when a is divided by a fixed positive int d.

Ex: if $d = 3$
$a = 10$ then $f(10) = 10 \text{ div } 3 = 3$
since $10 = 3 \times 3 + 1$.

if $a = -10$ then $f(-10) = -10 \text{ div } 3 = -4$
$d = 3$ $-10 = 3 \cdot (-4) + 2$

2) $g(a) = a \bmod d$ → takes int a and returns the int. remainder when $\frac{a}{d}$

if $a = 10$
$d = 3$ $\Rightarrow g(10) = 10 \bmod 3 = 1$.

One-to-one (injective):
if diff. ~~outputs~~ inputs always produce diff. outputs,
i.e. if $f(a_1) = f(a_2)$, then it must be that $a_1 = a_2$

Onto (surjective): $f(a) = y$.

1) $f(a) = a \text{ div } d$

one-to-one: No (unless $d = 1$)
onto: Yes

$g(a) = a \bmod d$
one-to-one: No (for $d > 1$)
onto: No, unless $d = 1$, in which case $a \bmod 1 = 0$ for all a, so it's not onto $\mathbb{Z}$.

Problem 7: Convert the decimal expansion of each of these integers to a binary expansion.

a) 231

231 | 2
1 115 | 2
1 57 | 2
1 28 | 2
0 14 | 2
0 7 | 2
1 3 | 2
1 1 | 2
1

11100111

b) 4532

4532 | 2
0 2266 | 2
0 1133 | 2
1 566 | 2
0 283 | 2
1 141 | 2
1 70 | 2
0 35 | 2
1 17 | 2
1 8 | 2
0 4 | 2
0 2 | 2
0 1

1000110110100

c) 97644

97644 | 2
0 48822 | 2
0 24411 | 2
1 12205 | 2
1 6102 | 2
0 3051 | 2
1 1525 | 2
1 762 | 2
0 381 | 2
1 190 | 2
0 95 | 2
1 47 | 2
1 23 | 2
1 11 | 2
1 5 | 2
1 2 | 2
0 1 | 2
1 0

10111011011100

Problem 8: Convert the binary exp. to a decimal exp-n.

a) (11111)

$(1\cdot 2^4)+(1\cdot 2^3)+(1\cdot 2^2)+(1\cdot 2^1)+(1\cdot 2^0) = 16+8+4+2-1 = 31.$

b) $(1000000001)_2 =$

$(1\cdot 2^9)+(0\cdot 2^8)+(0\cdot 2^7)+(0\cdot 2^6)+(0\cdot 2^5)+(0\cdot 2^4)+(0\cdot 2^3)+(0\cdot 2^2)+(0\cdot 2^1)+(1\cdot 2^0)$

$= 513$

c) $(10101010)_2 =$

$= 2^8+0+2^6+0+2^4+0+2^2+0+2^0 =$

$= 256+64+16+4+1 = 341.$

d) $(1101001000010000)_2$

$2^{14}+2^{13}+2^{11}+2^8+2^4 = 26896$

Problem 12 Use Euclidean algorithm to find.

a) gcd (12, 18)

$12 = 2 \cdot 3 \cdot 2 = 2^2 \cdot 3$
$18 = 2 \cdot 3 \cdot 3 = 2 \cdot 3^2$ $\Rightarrow (2 \cdot 3) = 6.$

b) gcd (111, 201)

$111 = 3 \cdot 37$
$201 = 3 \cdot 67$ $\Rightarrow (3 \cdot 37 \cdot 67) =$