Cryptography pset 2

1.

1.10. For each of the gcd(a, b) values in Exercise 1.9, use the extended Euclidean algorithm (Theorem 1.11) to find integers u and v such that $au + bv = \gcd(a, b)$.

(a) gcd(291, 252).

(b) gcd(16261, 85652).

Sol (a)

r_i	u_i	v_i
291	1	0
252	0	1
291 % 252 = 291 − 252 = 39	1 + 0(−1) = 1	0 + 1(−1) = −1
252 % 39 = 252 − 6.39 = 18	0 + 1(−6) = −6	1 + (−1)(−6) = 7
39 % 18 = 39 − 2.18 = 3	1 − 2(−6) = 13	−1 − 2(7) = −15
18 % 3 = 18 − 6.3 = 0	− − −	− − − −

$\Rightarrow 291(13) + 252(-15) = \gcd(291, 252) = \boxed{3}$ Ans

$\Rightarrow \boxed{u = 13, \quad v = -15}$

(b)

r_i	u_i	v_i
16261	1	0
85652	0	1
16261 % 85652 = 16261	1	0
85652 % 16261 = 85652 − 5.16261 = 4347	0 − 5(1) = −5	1 − 5(0) = 1
16261 % 4347 = 16261 − 3.4347 = 3220	1 − 3(−5) = 16	0 + 1(−3) = −3
4347 % 3220 = 4347 − 3220 = 1127	−5 − 16 = −21	1 − (−3) = 4
3220 % 1127 = 3220 − 2.1127 = 966	16 − 2(−21) = 58	−3 − 2(4) = −11
1127 % 966 = 1127 − 966 = 161	−21 − 58 = −79	4 − (−11) = 15
966 % 161 = 966 − 6.161 = 0	− − −	− − −

$\Rightarrow \boxed{u = -79, \quad v = 15}$

here,
$a = 16261$
$b = 85652$

$\gcd(16261, 85652) = 16261(-79) + 85652(15) = \boxed{161}$

2.

1.15. Let $m \geq 1$ be an integer and suppose that

$$a_1 \equiv a_2 \pmod{m} \qquad \text{and} \qquad b_1 \equiv b_2 \pmod{m}.$$

Prove that

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m} \qquad \text{and} \qquad a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}.$$

(This is Proposition 1.13(a).)

Sol

$a_1 \equiv a_2 \pmod{m} \implies a_1 = mk_a + a_2$

$b_1 \equiv b_2 \pmod{m} \implies b_1 = mk_b + b_2$

$a_1 \pm b_1 = (mk_a + a_2) \pm (mk_b + b_2)$.

$= m(k_a \pm k_b) + (a_2 \pm b_2)$

As we know that m divides $m(k_a \pm k_b)$, we can say...

$\boxed{a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}}$, Hence Proved

Moreover, $a_1 b_1 = (mk_a + a_2)(mk_b + b_2)$

$= m^2 k_a k_b + mk_a b_2 + mk_b a_2 + a_2 b_2$

As we know that m divides $m^2 k_a k_b$, $mk_a b_2$ and $mk_b a_2$

we can say, $a_1 b_1 = m\underbrace{(mk_a k_b + k_a b_2 + k_b a_2)}_{\text{if treated as quotient}} + a_2 b_2$

$\Rightarrow \boxed{a_1 b_1 = a_2 b_2 \pmod{m}}$, Hence Proved

3. The previous problem shows that congruence modulo m is "compatible with" addition and multiplication, in a suitable sense. In this problem, you'll see that this is **not** true of other arithmetic operations, so you have to be careful.

   (a) (Congruence is not compatible with powers) Suppose we work modulo 11. It is tempting to think that "if $e \equiv f \mod 11$, then $2^e \equiv 2^f \pmod{11}$." Find a counterexample showing that this is false (give specific values of e and f and explain why they give a counterexample).

   (b) (Congruence is not compatible with division) Suppose that we work modulo 21. It is tempting to think that we can "cancel common factors" in a congruence. For example, one might guess that "if $2x \equiv 12 \pmod{34}$, then $x \equiv 6 \pmod{34}$." Find a counterexample (a specific value of x) showing that this is false, and briefly explain why it is a counterexample.

Note: we'll see later that we can recover a sort of compatibility with both powers and division, but the details are subtle.

Sol. (a) "if $e \equiv f \bmod 11$ then $2^e \equiv 2^f \pmod{11}$" $\Leftarrow$ statement

$\Rightarrow$ $\boxed{e = 11k + f}$ then the statement says $2^{11k+f} \equiv 2^f \pmod{11}$

if we take $k = 1$ and $f = 0$, the equation gives...
$e = 11(1) + 0 = 11$ and
in order to statement to be true, $2^{11} \equiv 2^0 \pmod{11}$
$\Rightarrow$ $2048 \equiv 1 \pmod{11}$ which is False because
$2048 \% 11 = 2$, Hence this is a valid counterexample

(b) "if $2x = 12 \pmod{34}$, then $x \equiv 6 \pmod{34}$" $\Leftarrow$ statement
$\Rightarrow$ $\boxed{2x = 34k + 12}$ $\forall k$, then the statement says
that $(17k + 6) \equiv 6 \pmod{34}$
thus, $17k + 6 = 34k' + 6$ $\Rightarrow$ $k = 2k'$ where $k, k' \in \mathbb{Z}$
But, in the case when $k =$ odd (for eg. 3), then k' would not be an integer (which shouldn't be the case)
$\Rightarrow$ $x = 17k + 6 = 17(2) + 6 = \boxed{40}$ (Hence, this is a valid counterexample)

4. Prove the following basic facts about congruence, asserted in class.

(a) For any integer $a \in \mathbb{Z}$ and positive integer m, $a \equiv (a\%m) \pmod{m}$.

(b) With a, m as above, the number $a\%m$ is the *unique* element of $\{0, 1, \cdots, m-1\}$ that is congruent to a modulo m (that is, no other element of this set is congruent to a modulo m).

(c) For any two integers $a, b \in \mathbb{Z}$ and any positive integer m, $a \equiv b \pmod{m}$ *if and only if* $a\%m = b\%m$.

Sol

(a) If we divide two positive integers a and m, let's say we get remainder r and quotient q

∴ Then, $(a = mq + r)$

$\Rightarrow$ To prove: $a \equiv (a\%m) \pmod{m}$

$\Rightarrow (mq+r) \equiv r \pmod{m}$

thus, $(mq+r)$ can be represented as $(mk+r)$

and as these must represent the same number,

$mq+r = mk+r \Rightarrow q = k$. , Hence Proved. ∎

(b) $\boxed{a = mq+r}$, if $r > m$, then $\exists k$ such that $r - km = r' \geq 0$, $(r' < m)$

$\Rightarrow a = mq + r = mq + (km + r') = m(q+k) + r'$.

$\Rightarrow a\%m = r'$ where $r' \in \{0, 1, \ldots, m-1\}$

if $r < m$, then $a\%m = r$, where $r \in \{0, 1, \ldots, m-1\}$

Hence Proved. ∎ Now we need to prove it's uniqueness

proof

uniqueness:

if $a \equiv r \pmod{m}$

and $0 \leq r < m$

then $r = a\%m$

$a = r + km$

$a = (a\%m) + \lfloor \frac{a}{m} \rfloor m$ (by definition)

$\Rightarrow \frac{a}{m} = \frac{r}{m} + k$

$\Rightarrow \frac{a}{m} = \frac{(a\%m)}{m} + \lfloor \frac{a}{m} \rfloor$

[dividing equation by m]

As we know that the lefthand sides of both equations are equal, then the right hand sides should also equate $\Rightarrow \frac{r}{m} + k = \frac{(a\%m)}{m} + \lfloor \frac{a}{m} \rfloor$

As we know, k & $\lfloor \frac{a}{m} \rfloor$ are integers and $\frac{r}{m}$ and $\frac{(a\%m)}{m}$ are between 0 and 1, Integral & fractional parts should equate separately ... $\Rightarrow \boxed{r = a\%m}$, Hence Proved ∎

(c) To prove: $a \equiv b \pmod{m} \Leftrightarrow a\%m = b\%m$

(i) direction "$\Rightarrow$": $a \equiv b \pmod{m} \Rightarrow a = mq + b$

$\Rightarrow a\%m = (mq+b)\%m = \boxed{b\%m}$, Hence Proved

(ii) direction "$\Leftarrow$": $a\%m = b\%m \Rightarrow \begin{pmatrix} a = mq_1 + r \\ b = mq_2 + r \end{pmatrix}$, where $r < m$

$a - b = m(q_1 - q_2) \Rightarrow m \mid (a-b)$ which is definition of $a \equiv b \pmod{m}$, Hence Proved ∎

1.16. Write out the following tables for $\mathbb{Z}/m\mathbb{Z}$ and $(\mathbb{Z}/m\mathbb{Z})^*$, as we did in Figs. 1.4 and 1.5.

(a) Make addition and multiplication tables for $\mathbb{Z}/3\mathbb{Z}$.
(b) Make addition and multiplication tables for $\mathbb{Z}/6\mathbb{Z}$.
(c) Make a multiplication table for the unit group $(\mathbb{Z}/9\mathbb{Z})^*$.

Sol

(a)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(b)

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(c)

$\cdot$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

6.

1.19. Suppose that $g^a \equiv 1 \pmod{m}$ and that $g^b \equiv 1 \pmod{m}$. Prove that

$$g^{\gcd(a,b)} \equiv 1 \pmod{m}.$$

Sol

According to the extended Euclidean Algorithm, $\exists\, u, v \in \mathbb{Z}$ satisfying $au + bv = \gcd(a,b)$. Then,

$$g^{\gcd(a,b)} = g^{au+bv} = (g^a)^u \cdot (g^b)^v$$

By using the results, $\left.\begin{array}{l} g^a \equiv 1 \pmod{m} \\ g^b \equiv 1 \pmod{m} \end{array}\right\}$ from the question prompt

$$g^{\gcd(a,b)} = (g^a)^u \cdot (g^b)^v \equiv \boxed{1 \pmod{m}}$$, Hence Proved.