CISS451/MATH451: Cryptography and Computer Security
Assignment 4

This is an assignment on the congruence notation.

Here are some facts about $(\mathbb{Z}, +, \cdot, 0, 1)$. In the following x, y, z are integers, i.e. $x, y, z \in \mathbb{Z}$.

RING1: $x, y \in \mathbb{Z}$ can be replaced by $x + y \in \mathbb{Z}$

RING2: $(x + y) + z$ can be replaced by $x + (y + z)$

RING3: $x + (y + z)$ can be replaced by $(x + y) + z$

RING4: $x + 0$ can be replaced by x

RING5: x can be replaced by $x + 0$

RING6: $0 + x$ can be replaced by x

RING7: x can be replaced by $0 + x$

RING8: There is some $-x \in \mathbb{Z}$ such that $x + (-x)$ can be replaced by 0.

RING8B: There is some $-x \in \mathbb{Z}$ such that 0 can be replaced by $x + (-x)$.

RING9: There is some $-x \in \mathbb{Z}$ such that $(-x) + x$ can be replaced by 0.

RING9B: There is some $-x \in \mathbb{Z}$ such that 0 can be replaced by $(-x) + x$.

RING10: $x + y$ can be replaced by $y + x$.

RING11: $x, y \in \mathbb{Z}$ can be replaced by $xy \in \mathbb{Z}$

RING12: $(xy)z$ can be replaced by $x(yz)$

RING13: $x(yz)$ can be replaced by $(xy)z$

RING14: $x1$ can be replaced by x

RING15: x can be replaced by $x1$

RING16: $1x$ can be replaced by x

RING17: x can be replaced by $1x$

RING18: $x(y + z)$ can be replaced by $xy + xz$

RING19: $xy + xz$ can be replaced by $x(y + z)$

RING20: $(y + z)x$ can be replaced $yx + zx$

RING21: $yx + zx$ can be replaced $(y + z)x$

RING22: xy can be replaced by yx

RING23: $xy = 0$ can be replaced by $[x = 0 \text{ or } y = 0]$.

The following are a notational rewrite rules for subtraction (i.e. the following are definitions and not axioms):

RING24: $x - y$ can be replaced by $x + (-y)$

RING25: $x + (-y)$ can be replaced by $x - y$

The following are from Theorems 1 and 2 proven in Assignment 1 (i.e. $0x = 0 = x0$)

TH1A: $0x$ can be replaced by 0

TH1B: 0 can be replaced by $0x$

TH1C: 0 can be replaced by $x0$

TH1D: $x0$ can be replaced by 0

TH1E: $0x$ can be replaced by $x0$

TH1F: $x0$ can be replaced by $0x$

Here are some facts from Theorem 3 (i.e. $x + y = 0 \implies y = -x$ and $y + x \implies y = -x$):

TH3A: If $x + y = 0$, then y can be rewritten as $-x$.

TH3B: If $x + y = 0$, then $-x$ can be rewritten as y.

TH3C: If $y + x = 0$, then y can be rewritten as $-x$.

TH3D: If $y + x = 0$, then $-x$ can be rewritten as y.

Here are some facts from Theorem 4 from Assignment 1:

TH4A: $-(-x)$ can be rewritten as x.

TH4B: x can be rewritten as $-(-x)$.

Here's Theorem 5 from Assignment 2 (i.e. $-1 \cdot x = -x = x \cdot (-1)$):

TH5A: $-1 \cdot x$ can be replaced by $-x$

TH5B: $-x$ can be replaced by $-1 \cdot x$

TH5C: $-x$ can be replaced by $x \cdot (-1)$

TH5D: $x \cdot (-1)$ can be replaced by $-x$

Here's Theorem 6 from Assignment 2 (i.e. $(-y)x = -(yx) = y(-x)$):

TH6A: $(-y)x$ can be replaced by $-(yx)$

TH6B: $-(yx)$ can be replaced by $(-y)x$

TH6C: $-(yx)$ can be replaced by $y(-x)$

TH6D: $y(-x)$ can be replaced by $-(yx)$

TH6E: $(-y)x$ can be replaced by $y(-x)$

TH6F: $y(-x)$ can be replaced by $(-y)x$

Here's Theorem 7 from Assignment 2 (i.e. $(-x)(-y) = xy$ and $(-1)(-1) = 1$):

TH7A: $(-x)(-y)$ can be replaced by xy

TH7B: xy can be replaced by $(-x)(-y)$

TH7C: $(-1)(-1)$ can be replaced by 1

TH7D: 1 can be replaced by $(-1)(-1)$

Here's Theorem 8 ($0 = -0$):

TH8A: 0 can be replaced by -0

TH8B: -0 can be replaced by 0

Here's Theorem 9 (the additive cancellation property):

TH9A: If $a + x = a + y$, then x can be replaced by y.

TH9B: If $x + a = y + a$, then x can be replaced by y.

Here's Theorem 10 (the multiplicative cancellation property):

TH9A: If $ax = ay, a \neq 0$, then x can be replaced by y.

TH9B: If $xa = ya, a \neq 0$, then x can be replaced by y.

Now for stuff on divisibility.

Here are the "rewrite rules" for the definition of "divisibility":

DIV1: $d \mid a$ can be replaced by $[dx = a$ for some $x \in \mathbb{Z}]$

DIV2: $[dx = a$ for some $x \in \mathbb{Z}]$ can be replaced by $d \mid a$

which are really the same as:

DIV1: $d \mid a$ can be replaced by $[\exists x \in \mathbb{Z}(dx = a)]$

DIV2: $[\exists x \in \mathbb{Z}(dx = a)]$ can be replaced by $d \mid a$

Here's Theorem 11 and 12:

THM12A: $a \mid a$.

THM12B: If $a \mid b$ and $b \mid c$, then $a \mid c$.

Here's Theorem 13 (a whole mouthful of it ...)

THM13A: $1 \mid a$.

THM13B: $-1 \mid a$.

THM13C: If $d \mid a$, then $-d \mid a$

THM13D: If $d \mid a$, then $d \mid ax$

THM13E: If $d \mid a$ and $d \mid b$, then $d \mid (a + b)$.

THM13F: Given integers x and y, if $d \mid a$ and $d \mid b$, then $d \mid (ax + by)$.

Theorem Foil:

Thm Foil A.)
$(w+x)(y+z)$ can be replaced by $(wy+wz)+(xy+xz)$

$$\begin{aligned}(w+x)(y+z) &= (w(y+z)+x(y+z)) && \text{by RING20}\\ &= (wy+wz)+(xy+xz) && \text{by RING18}\end{aligned}$$

Thm Foil B.)
$(w+x)(y+z)$ can be replaced by $(wy+xy)+(wz+xz)$

$$\begin{aligned}(w+x)(y+z) &= ((w+x)y+(w+x)z) && \text{by RING18}\\ &= (wy+xy)+(wz+xz) && \text{by RING18}\end{aligned}$$

Theorem Brandy1:

Thm Brandy1A.)
$a=(b+c)$ can be replaced by $a-c=b$

$$\begin{aligned}a &= (b+c)\\ a+-c &= (b+c)+-c\\ a+-c &= b+(c+-c) && \text{by RING2}\\ a+-c &= b+0 && \text{by RING8}\\ a+-c &= b && \text{by RING4}\\ a-c &= b && \text{by RING25}\end{aligned}$$

Thm Brandy1B.)
$a=(b+c)$ can be replaced by $a-b=c$

$$\begin{aligned}a &= (b+c)\\ a+-b &= -b+(b+c)\\ a+-b &= (-b+b)+c && \text{by RING3}\\ a+-b &= 0+c && \text{by RING9}\\ a+-b &= c && \text{by RING4}\\ a-b &= c && \text{by RING25}\end{aligned}$$

Thm Brandy1C.)
$(a + b) = c$ can be replaced by $b = c - a$

$$\begin{aligned}
(a + b) &= c \\
-a + (a + b) &= c + -a \\
(-a + a) + b &= c + -a && \text{by RING3} \\
0 + b &= c + -a && \text{by RING9} \\
b &= c + -a && \text{by RING4} \\
b &= c - a && \text{by RING25}
\end{aligned}$$

Thm Brandy1D.)
$(a + b) = c$ can be replaced by $a = c - b$

$$\begin{aligned}
(a + b) &= c \\
(a + b) + -b &= c + -b \\
a + (b + -b) &= c + -b && \text{by RING2} \\
a + 0 &= c + -b && \text{by RING8} \\
a &= c + -b && \text{by RING4} \\
a &= c - b && \text{by RING25}
\end{aligned}$$

Here are some questions on GCD.

For the following we will assume that you have access to tables or a computer that can compute only integer quotients and remainders, i.e., that you have access to a Euclidean property machine. For instance, if you're given 100 and 23 and you want want to find q, r such that

$$100 = 23 \cdot q + r, \;\; 0 \leq r < 23$$

you can of course compute q and r using C++ like this:

```
std::cout << 100 / 23 << ',' << 100 % 23 << '\n';
```

You can do this in Python:

```
print divmod(100, 23)
```

Q1.

(a) Write down the prime factorization of 123556.

(b) Write down the prime factorization of 5436.

(c) Compute gcd$(123556, 5436)$ using the above prime factorizations.

Here's an example of how you must present your prime factorization:

$$300 = 2^2 \cdot 3^1 \cdot 5^2$$

SOLUTION.

a) $123556 = 2^2 \cdot 17^1 \cdot 23^1 \cdot 79^1$

b) $5436 = 2^2 \cdot 3^2 \cdot 151^1$

c) $gcd(123556, 5436) = 2^2 = 4$

Q2. Write a list of Euclidean computations to compute the $\gcd(123556, 5436)$. The last remainder must be 0.

(If you don't know what I'm talking about, then you have not read the notes I gave you. Read it.)

SOLUTION.

$123556 = 5436 \cdot 22 + 3964$
$5436 = 3964 \cdot 1 + 1472$
$3964 = 1472 \cdot 2 + 1020$
$1472 = 1020 \cdot 1 + 425$
$1020 = 425 \cdot 2 + 116$
$425 = 116 \cdot 3 + 104$
$116 = 104 \cdot 1 + 12$
$104 = 12 \cdot 8 + 8$
$12 = 8 \cdot 1 + 4$
$8 = 4 \cdot 2 + 0$

So 4 is the gcd(123556, 5436)

Q3. Find integers x and y such that

$$123556x + 5436y = \text{gcd}(123556, 5436)$$

You should begin with labeling all the Euclidean computations from Q2 and then perform substitutions. Make sure you indicate very clearly which equation you're using. Here's a reminder on how to label equations:

$$1 + 1 = 2 \tag{1}$$

SOLUTION.

$(12 \cdot 1) + (8 \cdot -1) = 4$
$(12 \cdot 1) + ((104 \cdot 1) + (12 \cdot -8)) - 1 = 4$
$(12 \cdot 9) + (104 \cdot -1) = 4$
$((116 \cdot 1) + (104 \cdot -1))9 + (104 \cdot -1) = 4$
$(116 \cdot 9) + (104 \cdot -10) = 4$
$(116 \cdot 9) + ((425 \cdot 1) + (116 \cdot -3)) - 10 = 4$
$(116 \cdot 39) + (425 \cdot -10) = 4$
$((1020 \cdot 1) + (425 \cdot -2))39 + (425 \cdot -10) = 4$
$(1020 \cdot 39) + (425 \cdot -88) = 4$
$(1020 \cdot 39) + ((1472 \cdot 1) + (1020 \cdot -1)) - 88 = 4$
$(1020 \cdot 127) + (1472 \cdot -88) = 4$
$((3964 \cdot 1) + (1472 \cdot -2))127 + (1472 \cdot -88) = 4$
$(3964 \cdot 127) + (1472 \cdot -342) = 4$
$(3964 \cdot 127) + ((5436 \cdot 1) + (3964 \cdot -1)) - 342 = 4$
$(3964 \cdot 469) + (5436 \cdot -342) = 4$
$((123556 \cdot 1) + (5436 \cdot -22))469 + (5436 \cdot -342) = 4$
$(123556 \cdot 469) + (5436 \cdot -10660) = 4$

$123556x + 5436y = gcd(123556, 5436) = 4$

So $x = 469$ and $y = -10660$.

Q4. Show that if you have the following equations:

$$c_1r_0 + d_1r_1 = r_3 \tag{1}$$
$$c_2r_0 + d_2r_1 = r_4 \tag{2}$$
$$r_3 + (-q_4)r_4 = r_5 \tag{3}$$

Show that

$$(c_1 - q_4c_2)r_0 + (d_1 - q_4d_2)r_1 = r_5$$

For this question, you need not quote the RING properties/axioms or theorems, i.e., just treat this as a "normal" algebra manipulation problem.

SOLUTION.

$c_1r_0 + d_1r_1 + (-q_4)r_4 = r_5$
$(c_1r_0 + d_1r_1) + (-q_4)(c_2r_0 + d_2r_1) = r_5$
$(c_1r_0 + d_1r_1) + ((-q_4)c_2r_0 + (-q_4)d_2r_1) = r_5$
$(c_1r_0 - q_4c_2r_0) + (d_1r_1 - q_4d_2r_1) = r_5$
$\therefore\ (c_1 - q_4c_2)r_0 + (d_1 - q_4d_2)r_1 = r_5$

Now for the rewrite rules for the congruence notation for modular arithmetic:

CON1: $a \equiv b \pmod{n}$ can be replaced by $n \mid (a - b)$

CON2: $n \mid (a - b)$ can be replaced by $a \equiv b \pmod{n}$

If $a \equiv b \pmod{n}$ then we say "a is congruent to b mod n".

Theorem 14. *Let a, n be integers with $n > 0$. $a \equiv 0 \pmod{n}$ iff $n \mid a$*

This is easy to prove. I'll do this one for you quickly. If $a \equiv 0 \pmod{n}$, then by definition (make sure you check that I'm not lying!), n divides $a - 0$, i.e. n divides a. And if n divides a, then n divides $a - 0$, and therefore $a \equiv 0 \pmod{n}$.

You might want to write it out in full. Note that I used the fact that a is the same as $a - 0$. (Is this true? Are you sure? Don't say I didn't warn you.)

Theorem 15.

(a) $a \equiv a \pmod{n}$

(b) $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$

(c) $a \equiv b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$

These are called (respectively) the reflexive, symmetric, and transitive properties of the congruence relation. "$a \equiv b \equiv c \pmod{n}$" means

$$\begin{aligned} a &\equiv b \pmod{n} \\ b &\equiv c \pmod{n} \end{aligned}$$

By the way, there are lots of relations which are reflexive, symmetric, and transitive. For example, if the universe is the set of all lines in 2-d space, then the relation "is parallel to" is reflexive, symmetric, and transitive. Is $<$ on real numbers reflexive? symmetric? transitive?

How about the "is married to" relation on people?

How about "feeds on" relations in the food web?

Q5. Prove Theorem 15(c).

SOLUTION.

"$a \equiv b \equiv c \pmod{n}$ means

$$\begin{aligned}
a &\equiv b \pmod{n} \\
n &\mid a - b && \text{by CON1} \\
nx &\equiv a - b && \text{by DIV1} \\
nx - -b &\equiv a && \text{by Thm Brandy1A} \\
nx + b &\equiv a && \text{by THM4A}
\end{aligned}$$

and

$$\begin{aligned}
b &\equiv c \pmod{n} \\
n &\mid b - c && \text{by CON1} \\
ny &\equiv b - c && \text{by DIV1} \\
nx - b &\equiv -c && \text{by Thm Brandy1B}
\end{aligned}$$

$$\begin{aligned}
(nx + b) + (ny + -b) &\equiv a + (-c) \\
nx + (b + ny + -b) &\equiv a + (-c) && \text{by RING2} \\
nx + (b + ny) + -b &\equiv a + (-c) && \text{by RING3} \\
nx + (ny + b) + -b &\equiv a + (-c) && \text{by RING10} \\
(nx + ny) + (b + -b) &\equiv a + (-c) && \text{by RING2 and RING3} \\
(nx + ny) + (0) &\equiv a + (-c) && \text{by RING8} \\
(nx + ny) &\equiv a + (-c) && \text{by RING4} \\
n(x + y) &\equiv a + (-c) && \text{by RING19} \\
n(x + y) &\equiv a - c && \text{by RING24} \\
n &\mid a - c && \text{by DIV2} \\
\therefore \quad a &\equiv c \pmod{n} && \text{by CON2}
\end{aligned}$$

Theorem 16. *Let $n > 0$ and a, b, c, d be integers. If*

$$a \equiv b \pmod{n}$$
$$c \equiv d \pmod{n}$$

then

$$a + c \equiv b + d \pmod{n}$$

Q6. Prove Theorem 16.

SOLUTION.

From $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ we have:

$$
\begin{aligned}
n &\mid (a-b) && \text{by CON1} \\
&\text{and} \\
n &\mid (c-d) && \text{by CON1} \\
nx &\equiv (a-b) && \text{by DIV1} \\
&\text{and} \\
ny &\equiv (c-d) && \text{by DIV1} \\
nx + ny &\equiv (a-b) + (c-d) \\
\therefore \quad n(x+y) &\equiv (a-b) + (c-d) && \text{by RING19} \\
\therefore \quad n(x+y) &\equiv (a+(-b)) + (c+(-d)) && \text{by RING24} \\
\therefore \quad n(x+y) &\equiv a + (-b + (c + -d)) && \text{by RING2} \\
\therefore \quad n(x+y) &\equiv a + ((-b + c) + -d) && \text{by RING3} \\
\therefore \quad n(x+y) &\equiv a + ((c + -b) + -d) && \text{by RING10} \\
\therefore \quad n(x+y) &\equiv a + (c + (-b + -d)) && \text{by RING2} \\
\therefore \quad n(x+y) &\equiv (a+c) + (-b + -d) && \text{by RING3} \\
\therefore \quad n(x+y) &\equiv (a+c) + (-b - d) && \text{by RING25} \\
\therefore \quad n(x+y) &\equiv (a+c) - (b+d) && \text{by RING24} \\
\therefore \quad n &\mid (a+c) - (b+d) && \text{by DIV2} \\
\therefore \quad a+c &\equiv b+d && \text{by CON2}
\end{aligned}
$$

Theorem 17. *Let $n > 0$ and a, b, c, d be integers. Prove that if*

$$\begin{aligned} a &\equiv b \pmod{n} \\ c &\equiv d \pmod{n} \end{aligned}$$

then

$$ac \equiv bd \pmod{n}$$

Q7. Prove Theorem 17.

SOLUTION.

$$
\begin{aligned}
&n \mid a + -b && \text{by CON1} \\
&nx = a + -b && \text{by DIV1} \\
&nx - -b = a && \text{by Thm Brandy1B} \\
&nx + b = a && \text{by TH4A} \\
&\text{and} \\
&n \mid c + -d && \text{by CON1} \\
&ny = c + -d && \text{by DIV1} \\
&ny - -d = c && \text{by Thm Brandy1A} \\
&ny + d = c && \text{by TH4A}
\end{aligned}
$$

$$
\begin{aligned}
(nx + b) \cdot (ny + d) &= ac \\
n^2xy + nxd + nyb + bd &= ac && \text{by Thm Foil} \\
n^2xy + nxd + nyb &= ac + -bd && \text{by Thm Brandy1D} \\
n(nxy + xd + yb) &= ac + -bd && \text{by RING19} \\
n(nxy + xd + yb) &= ac - bd && \text{by RING25} \\
n &\mid ac - bd && \text{by DIV2} \\
\therefore \quad ac &\equiv bd && \text{by CON2}
\end{aligned}
$$

Q8.

(a) What is the ones digit (or the unit digit) of

$$1^{100} \cdot 2^{100} \cdot 3^{100} \cdot 4^{100} \cdot 5^{100}$$

(b) What about this one:

$$5^{1000} \cdot 11^{1000} \cdot 13^{1000} \cdot 17^{1000} \cdot 19^{1000}$$

(c) And this:

$$23^{10000} + 29^{10000} + 31^{10000} + 37^{10000} + 43^{10000}$$

(d) ... one last one [extra credit]:

$$123^{234^{345^{456^{567^{678^{789}}}}}}$$

Justify all your work. Writing down the final answer give you a zero. Nada. Zilch. I'm looking for a creative using of mathematical facts rather than trying to use a supercomputer to do the number crunching for you.

SOLUTION.

a)
$1^{100} = 1$

$2^{10} = 1024 \equiv 4 \pmod{10}$
$2^{100} = 4^{10} = 1048576 \equiv 6 \pmod{10}$

$3^4 = 81 \equiv 1 \pmod{10}$
$3^{100} = 3^{4^{25}} = 1^{25} \equiv 1 \pmod{10}$

$4^1 = 4$ and $4^2 = 16 \equiv 6 \pmod{10}$ this continues so evens end in 6 and odds end in 4
$4^{100} \equiv 6 \pmod{10}$

$5^1 = 5 \equiv 5 \pmod{10}$
this continues all these end in 5 $5^{100} \equiv 5 \pmod{10}$

Altogether $1 \cdot 6 \cdot 1 \cdot 6 \cdot 5 = 180 \equiv 0 \pmod{10}$
So the last digit is a zero.

b)
$5^{1000} \equiv 5 \pmod{10}$

$11^1 = 11 \equiv 1 \pmod{10}$
$11^{1000} \equiv 1 \pmod{10}$

$13^1 \equiv 3$ so 13 behaves lik 3 $3^4 = 81 \equiv 1 \pmod{10}$
$13^{1000} \equiv 1 \pmod{10}$

$17^1 \equiv 7$ so 17 behaves lik 7 $7^4 = 2401 \equiv 1 \pmod{10}$
$17^{1000} \equiv 1 \pmod{10}$

$19^1 \equiv 9$ so 19 behaves lik 9 $9^2 = 81 \equiv 1 \pmod{10}$
$19^{1000} \equiv 1 \pmod{10}$

Altogether $5 \cdot 1 \cdot 1 \cdot 1 \cdot 1 = 5 \equiv 5 \pmod{10}$
So the last digit is a 5.

c)
$23^1 \equiv 3$ so 23 behaves lik 3 $3^4 = 81 \equiv 1 \pmod{10}$
$23^{1000} \equiv 1 \pmod{10}$

$29^1 \equiv 9$ so 29 behaves lik 9 $9^2 = 81 \equiv 1 \pmod{10}$
$29^{1000} \equiv 1 \pmod{10}$

$31^1 \equiv 1$ so 31 behaves like 1
$31^{1000} \equiv 1 \pmod{10}$

$37^1 \equiv 7$ so 37 behaves like 7 $7^4 = 2401 \equiv 1 \pmod{10}$
$37^{1000} \equiv 1 \pmod{10}$

$43^1 \equiv 3$ so 43 behaves lik 3 $3^4 = 81 \equiv 1 \pmod{10}$
$43^{1000} \equiv 1 \pmod{10}$

Altogether $1+1+1+1+1=5 \equiv 5 \pmod{10}$
So the last digit is a 5.

d)
$123^{234} = 123^{4^{58}} \cdot 123^2$
$1^{58} \cdot 123^2 = 123^2$
$123 \equiv 3 \pmod{10}$ so $123^2 \equiv 3^2 = 9$
$9^{345} \equiv 9$ because 345 is odd
$9^{456} \equiv 1$ because 456 is even
$1^{678^{789}} \equiv 1 \pmod{10}$

So $123^{234^{345^{456^{567^{678^{789}}}}}} \equiv 1 \pmod{10}$