# Homework 1

Erik Brakke

September 10, 2015

**Collaborators: Alison Kendler**

## Answer 1

(a) Thm: $(a_1 \equiv a_2)$ if and only if $b \mid (a_1 - a_2)$
Proof: Assume $b \mid (a_1 - a_2)$
$b \mid (qb + r_1) - (qb + r_2)$ (by division with remainder fact)
$b \mid (qb - qb) + (r_1 - r_2)$ (Associative property)
$b \mid (r_1 - r_2)$
$(r_1 - r_2) = 0$ (by definition of divides)
$r_1 = r_2$ (by addition)
$a_1 \bmod b = a_2 \bmod b$ (definition of 'mod')
$a_1 \equiv a_2$ (by fact of congruency)
So given that $b \mid (a_1 - a_2)$ we know that $a_1 \equiv a_2$

Now, assume $a_1 \equiv a_2$
$a_1 - a_2 \equiv 0$ (using subtraction)
$(a_1 - a_2) \bmod b = 0 \bmod b$ (by fact of congruency)
$r_{a_1 - a_2} = 0 \bmod b$ (by definition of 'mod')
Therefore, $b \mid (a_1 - a_2)$ (by definition of divides)
It has been proven in both directions

□

(b) Thm: $a \bmod b \equiv a$
Proof: $r \equiv a$ (by definiton of 'mod')
$r \bmod b = a \bmod b$ (by fact about congruency)
$r \bmod b = r$ (by definition of 'mod')
$r = r$ because $r$ is the remainder, so $r \bmod b$ is just $r$
So, we have now that $r = r$ from $a \bmod b \equiv a$
Therefore, $a \bmod b \equiv a$ □

(c) Thm: $(a_1 \bmod b) + (a_2 \bmod b) \equiv a_1 + a_2$ and $(a_1 \bmod b)(a_2 \bmod b) \equiv a_1 a_2$
Proof: We know, $a \bmod b \equiv a$ (by proof in (b))
Using this knowledge, we can rewrite both congruencies as: $a_1 + a_2 \equiv a_1 + a_2$ and $a_1 a_2 \equiv a_1 a_2$ (substitution)
Therefore, we have shown the theorm is true

□

(d) Thm: $-a \equiv b - a$
Proof: We know that $a_1 \equiv a_2$ if and only if $b \mid (a_1 - a_2)$ (using proof from part (a))
Let $a_1 = -a$ and $a_2 = (b - a)$
So, we have to show that $b \mid (-a - (b - a))$
This reduces to $b \mid -b$
$b$ does in fact divide $-b$ becuase there is no remainder $r$
Therefore, $-a \equiv b - a$ □

(e) $246^{16}$ mod $251 = -2^{16}$ mod $251$
$-2^{16}$ mod $251 = -2^8 * -2^8$ mod $251$
$256 * 256$ mod $251 = 5 * 5$ mod $251$
The answer is: $25$ mod $251$

## Answer 2

(a) $7^2$ mod $19 = 11$
$7^4$ mod $19 = 7^2$ mod $19 * 7^2$ mod $19 = 11 * 11$ mod $19 = 7$
$7^8$ mod $19 = 7^4$ mod $19 * 7^4$ mod $19 = 7^2$ mod $19 = 11$
$7^{16}$ mod $19 = 7^8$ mod $19 * 7^8$ mod $19 = 7$
I'm noticing the pattern...
$7^{32}$ mod $19 = 11$
$7^{64}$ mod $19 = 7$

(b) $7^{75}$ mod $19 = 7^{64}$ mod $19 * 7^8$ mod $19 * 7^2$ mod $19 * 7$ mod $19$
$(7 * 11 * 11 * 7)$ mod $19$ $7^2$ mod $19 * (7^2 * 7^2)$ mod $19$ because $11 = 7^2$ mod $19$
$11 * 7$ mod $19 = 1$

(c)
```
Def EfficientAlg($a, b, c$):
If $b = 0$: return 1
If $b = 1$: return $a$ mod $c$
Else:
If $b$ is even: return (EfficientAlg($a, b/2, c$) * EfficientAlg($a, b/2, c$)) mod $c$
If $b$ is odd: return ($a*$ EfficientAlg($a, b - 1, c$)) mod c
```
If memoization is used, this algorithm is very efficent.

## Answer 3

(a) Thm: For any integers $a \not\equiv 0, r, s$, if $ra \equiv sa$ then $r \equiv s$
Proof:
$ra - sa \equiv 0$ (subtraction)
$(ra - sa)$ mod $p = 0$ mod $p$ (by property of congruence)
This means that $p \mid (ra - sa)$ (by 1(a))
$p \mid a(r - s)$ (distributive property)
Therefore, $p \mid a$ or $p \mid (r - s)$ (by our definition of prime)
We know that $p \nmid a$ because $a \not\equiv 0$
Therefore, $(r - s) \equiv 0$ (property of divides)
Therefore, $r \equiv s$ (addition) □

(b) Thm: For any integer $a \not\equiv 0$, $a$ mod $p$, $2a$ mod $p$,...,$(p-1)$ mod p will hit every element in 1,2,3,...,$p-1$ exactly once
Proof:
First, let's assume that a number in the set {1,2...(p-1)} can be hit more than once
$\exists_{x,y} \in \{1, 2, ..., (p-1)\}, x \neq y$ such that $xa \equiv ya$
However, we have already proved that if $xa \equiv ya$ then $x \equiv a$ (by 3(a))
This is a contradiction, so a number cannot be hit more than once.

Now let's assume that a number cannot be hit.
$\exists_x \in \{1, 2, ..., (p-1)\}$ such that $\forall_y \in \{1, 2, ..., (p-1)\} xa \not\equiv y$
In order for this to be the case, $xa \equiv 0$ or $xa \equiv z$ where $z > p$ (The only numbers not in the set)

For $xa \equiv 0$
This means that $p \mid xa$, so $p \mid x$ or $p \mid a$
We know that $a \not\equiv 0$ therefore $p \mid x$
However, because $p$ is a prime number, there is no number $x$ in the set $\{1, 2, ..., (p-1)\}$ such that $p \mid x$ (By definition of prime number)

For $xa \equiv z$ where $z > p$
This is impossible, because $z$ mod $p$ is $r$ where $0 < r < p$ (fact about integer division)

Therefore, every number must be hit at least once.
I have proven that every number must be hit at least once, and at most once, therefore every number in the set $\{1, 2, ..., (p-1)\}$ is hit exactly once □

(c) Thm: $a \not\equiv 0 \pmod{p}$ then $a^{p-1} \equiv 1$
Proof:
Let's start by multiplying the values $a * 2a * 3a \dots (p-1)a$
Because we know that every element must be hit, this can be rewritten as $1 * 2 * \cdots * (p-1)$ or $(p-1)!$ (by 3(b))
We can also write it as $a^{p-1} * (p-1)!$ (by distributive property)
So we have that $a^{p-1} * (p-1)! \equiv (p-1)!$
Thus, $a^{p-1} \equiv 1$ (By the multiplicative identity) □

(d) FurMAH

(e) Thm: $\forall_a a \not\equiv 0( \text{ mod } p)$ then $\exists_b ab \equiv 1$
Proof:
We know that $a^{p-1} \equiv 1$ (Fermat's theorm)
We can rewrite this as $a * a^{p-2} \equiv 1$ (multiplying exponents with equivalent bases)
Now, we can just say that $b = a^{p-2}$
Therefore, the has to exist some $b$ where $ab \equiv 1$ for $a \not\equiv 0$ and some prime $p$
□

## Answer 4

Given a message space of size $s$, isolate it into the unique characters that exist in that message space.

Determine the size of this character set, $U$, order the characers, and assign each character an index $i$
Now for any message $m$, choose a uniformly random key $k$ that also exists in $s$. (keys should not be reused)
Now add each character's index from $m$ it's corrosponding character's index in $k$ modulo the size of $U$. This is cipher text $c$
The receiver then subtracts each character's index in $c$ from the character's index in $k$ modulo the size of $U$ to get $m$
The number of keys is exactly $s$, the number of possible messages that exist because you are chosing the key from this message space

Thm: This crypto system in perfectly secure

Proof: I will prove it is Shannon secure, which proves that it is perfectly secure
Shannon security states that $\Pr_{k \in K}[Enc_k(m_0) = c] = \Pr_{k \in K}[Enc_k(m_1) = c]$ for some $m_0, m_1 \in M$
Let's assume we don't have Shannon security

This would mean that given $c$, it is more likely to be $m_0$ than $m_1$, or vice versa
This would mean that for some index $i$, $m_0[i] + k[i] (\mod |U|) = c[i]$ is more likely than getting $c[i]$ from $m_1$ under a different random key $k$ (or vice versa)
However this could not be, because we have chosen the key $k$ at random for both $m_0$ and $m_1$, any resulting $c[i]$ from encrypting $m_0$ is just as likely to happen from encrypting $m_1$.
Therefore it is Shannon Seucre and from Thm 1 from the class notes, it is perfectly secure □

## Answer 5

(a) Their messages are not securly encrypted because they are using the same 96-bit-long pad. Because there is a common repitiion in the messages (namely that all messages will start with either a 'B' or an 'S') there will be the same repition in the encrypted messages as well because the pad $k$ is not changing. An attack could eventually learn that these correspond to $B$ and $S$

(b) Yes he can. For the same reasons as stated above, after recieving and analyzing some encrypted messages, Moe would could tell that the first bits of the cipher text are the encryption of $B$ or $S$. Furthermore, he would see that these bits are not changing, that is, the encryption of $B$ and $S$ are always the same. All Moe would have to do is change the first bits to the ecryption for the opposite action Bob wants to do. Alice would decrypt this message with no error and would proceed accordingly.

---

## References

None