CS70–Fall 2011 — Solutions to Homework 5

1. **Euclid's argument**
   Solution:
   Although Euclid's argument is valid, the given proof is not correct. In order to get a contradiction, Euclid assumes that there are only k primes $p1p2\cdots pk$. This false assumption helps him to show that $p1p2\cdots pk+1$ is a prime as well. However, there might be prime numbers beyond the first k. Lets take an example with $k=6$. Under this condition, we will have

   $$2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13+1=30031$$

   Under the assumption that $\{2,3,5,7,11,13\}$ are the only prime numbers, the number 30031 is also a prime, because none of the numbers in the list divides 30031. However, the assumption that $\{2,3,5,7,11,13\}$ are the only prime numbers is incorrect. In fact, there is a prime number 59 such that

   $$59\cdot 509=30031$$

   Because of the faulty assumption that there are only k prime numbers, the proof is incorrect.

2. **GCD**

   (a) Use extended euclids algorithm to find some pair of integers j, k such that $52j+15k=3$.
   Solution:
   1- Applying the algorithm,

   $$52-3(15)=7$$

   $$15-2(7)=1$$

   $$7-7(1)=0$$

2- Solving,

$$1 = 15 - 2(7)$$
$$= 15 - 2(52 - 3(15))$$
$$= 7 \cdot 15 + (-2) \cdot 52$$

Multiplying both sides by 3 gives

$$3 = 3 \cdot 7 \cdot 15 + 3(-2)52 = 21 \cdot 15 + (-6)52$$

So, $j = -6$ and $k = 21$

(b) If $gcd(m, x) > 1$, how many distinct elements are there?
Solution:
We already know that if $gcd(m, x) = 1$, then the set $\{mod(ax, m) : a \in \{0, 1, \cdots, m-1\}\}$ has m elements. We can use this proof to find the number of elements when $gcd(m, x) > 1$. We have,

$$ax \equiv y (\text{mod } m)$$

and,

$$ax - y = km$$

We want to find numbers (x', m') such that $gcd(x', m') = 1$. Then the number of distinct elements would be m'. This is possible if we divide both sides by $gcd(m, x)$, because this will remove the common factor from both sides. Let $d = gcd(m, x)$. We have,

$$a\frac{x}{d} - \frac{y}{d} = k\frac{m}{d}$$

Note that $gcd(\frac{x}{d}, \frac{m}{d}) = 1$. So the total number of elements when $gcd(m, x) > 1$ is

$$Numberofelements = \frac{m}{d} = \frac{m}{gcd(m, x)}$$

3. **Nonnegative Combinations**

(a) Find a nice representation.
Solution:
Let x and y be solution to the equation $mx + ny = k$. We know that x_{nice} is bounded to be between $0 \leq x < n$. In order words, this means

$$x_{nice} = x (\text{mod } n)$$

which means that

$$n \mid (x_{nice} - x)$$

or in other words, $x_{nice} - x$ is a multiple of n. So we can write

$$x_{nice} - x = an$$

where a is any integer. Also because x and y are inter-dependent, constraints on x will have some effect on y as well. You have to figure this out yourself. Essentially, we have

$$y_{nice} - y = -am$$

This implies,

$$mx_{nice} + ny_{nice} = m(x + an) + n(y - am) = mx + ny = k$$

Thus, we know that there exists at least a solution with $x_{nice} = x (\text{mod } n)$. However, we still have to show that only one such representation is possible.

For this, assume that there are two solutions (x, y) and (x', y'). So we have

$$mx + ny = mx' + ny'$$

$$m(x - x') = n(y' - y)$$

$$(y' - y) = \frac{m(x - x')}{n}$$

Because $gcd(m, n) = 1$, this implies that in order for $y' - y$ to be an integer, $n \mid (x - x')$ must hold. Because $0 \leq x, x' < n$. So $x - x' = 0$, and thus

$$x = x'$$

Because $x - x' = 0$, the above equation becomes

$$m(0) = n(y' - y)$$

$$y' - y = 0$$

$$y' = y$$

Hence, we've shown that there only one nice representation.

(b) Prove that the largest k that cannot be written as a non-negative integral sum of m and n is $mn - m - n$
Solution:
Following the hint, we will find the maximum possible ways of x and y. For x it is pretty evident that

$$max(x) = n - 1$$

A non-negative integral sum is a sum where $0 \leq x < n$ and $y \geq 0$. However, we are asked to find the largest k that can't be written as a non-negative integral sum. This implies that $y < 0$. Now the question. Given that $y < 0$, whats the maximum possible value of y. Obviously,

$$max(y) = -1$$

So, we have

$$mx + ny = m(n-1) + n(-1) = mn - m - n$$

4. **Binary GCD**

(a) Prove that for any positive integers d, x, and y, d divides $gcd(x, y)$ if and only if d divides x and d divides y.
Solution:
If $d \mid gcd(x, y)$, then

$$d = ax + by$$
$$1 = a(\frac{x}{d}) + b(\frac{y}{d})$$

Because $a, b \in Z$, the above equation holds if and only if $\frac{x}{d}, \frac{y}{d} \in Z$. Therefore, if $d \mid gcd(x, y)$, then $d \mid x$ and $d \mid y$. ✓

(b) Prove that if a and b are both even, then $gcd(a, b) = 2gcd(a/2, b/2)$.
Solution:
The definition of $gcd(a, b)$ says that $gcd(a, b) = d$ iff $d \mid a$ and $d \mid b$ and

$$ax + by = d$$

where $x, y \in Z$. Because both a and b are even, this implies that d is even as well(which implies that $2 \mid a, b, d$). So we have,

$$x(\frac{a}{2}) + y(\frac{b}{2}) = (\frac{d}{2})$$

Note that the above equation is consistent keeping into constraints mentioned in the question(a, b are even). So

$$gcd(\frac{a}{2}, \frac{b}{2}) = \frac{d}{2}$$

$$d = 2 \cdot gcd(\frac{a}{2}, \frac{b}{2})$$

and because $d = gcd(a, b)$

$$gcd(a, b) = 2 \cdot gcd(\frac{a}{2}, \frac{b}{2}) \checkmark$$

(c) Prove that if a is odd and b is even, then $gcd(a, b) = gcd(a, b/2)$.
Solution:
This proof is quite similar to part(b), except that a is odd here. We already know that if $gcd(a, b) = d$, we have

$$ax + by = d$$

$\forall x, y \in Z$. Because a is odd, and b is even, this means that $d = gcd(a, b)$ has to be odd. So, dividing b by 2 won't effect the gcd whatsoever. This implies,

$$ax + (\frac{b}{2})y = d$$

$$gcd(a, b) = gcd(a, \frac{b}{2}) \checkmark$$

(d) Prove that if a and b are both odd, then $gcd(a, b) = gcd((ab)/2, b)$ where we assume $a \geq b$
Solution:
As

$$gcd(a, b) = gcd(a - b, b)$$

Because both a and b are odd, this means that $a - b$ is even. So we have $gcd(even, odd)$, which resembles a lot like part(c) where,

$$gcd(a, b) = gcd(a, \frac{b}{2})$$

where a was even, but b was odd. So by using part(c), we can write

$$gcd(a - b, b) = gcd(\frac{a - b}{2}, b)$$

$$gcd(a, b) = gcd(\frac{a - b}{2}, b) \checkmark$$

(e) Design an efficient binary gcd algorithm that uses $O(log(max(a, b)))$ subtractions, halving, and parity tests.

```
int binary_gcd(int a, int b)
{
   if (a == 0)
   {
      /* return b here */
      return b;
   }
   /* if a is even */
   if ((a & 1) == 0) /* to check if a is even, because you
       can't use % */
   {
      /* if b is even */
      if ((b & 1) == 0) /* to check if a is even, because
          you can't use % */
      {
         /* if both a and b are even, we use part(b) */
         return 2 * binary_gcd(a / 2, b / 2);
         /* there's a better way than multiply and
             dividing by 2. Can you figure out what? */

      }
      /* if b is not even */
      else
      {
         /* part(c) can help us here */
         return binary_gcd(a / 2, b);
      }
   }
   /* if a is not even */
   else
   {
      /* but b is even */
      if ((b & 1) == 0)
      {
         /* again part(c) can help us here */
         return binary_gcd(b / 2, a);
      }
      /* if both a and b are odd */
      else
      {
         /* part(d) is helpful here */
         if (a > b)
```

```
        {
            return binary_gcd(((a - b) / 2), a);
        }
        else
        {
            return binary_gcd(((b - a) / 2), a);
        }
    }
  }
}
```

One important that's left to do is to see whether we've meet that constraint $O(log(max(a, b)))$. I'm not explaining it here, because it is a big subject. You should come and talk to me if you want to know why this is the complexity. You might like to see this, but you will have to go through a lot of detail to get to the conclusion, and thats not described in the wiki page.

5. **Easy RSA**
   Solution:
   Note that the reason the RSA is considered to be secure is because the factorization of product of two large primes is very difficult. When you decide to use a single prime, you're in trouble.

   Suppose that we wish to send the message x. This is plain-text, and we encrypt in using our modified RSA scheme. So, the encrypted message y becomes

   $$y = E(x) \equiv x^e (\text{mod } p)$$

   So, Eve observes $y = x^e (\text{mod } p)$ as well as the numbers p and e. Now that she wishes to decrypt it, she'd use the RSA decryption function, which is

   $$x = D(y) \equiv x^{ed} (\text{mod } p)$$

   We already know that $ed \equiv 1(\text{mo d}p - 1)$. So Eve can follow the following scheme to find the plain-text x

   (a) Because $ed \equiv 1(\text{mod } p - 1)$, d is the multiplicative inverse of $e(\text{mod } p - 1)$. So, find d using the extended euclidean algorithm.

   (b) Compute $y^d (\text{mod } p)$ by whatever method you know. However, Repeated Squaring is considered to be the most efficient one.

In this way, you'll be able to extract the original contents from the encrypted message.

6. **RSA**
   Solution:
   Given $N = pq$ and $\phi(N) = (p-1)(q-1)$, we have to solve for p and q. Take $q = N/p$, and substitute in the second equation. I leave the algebra up to you, but at the end you should have something which looks like
   $$p^2 + (\phi(N) - N - 1)p + N$$
   Using the quadratic equation, solve for p and from the value of p, solve for q because $q = N/p$. Note that you'll get two solutions for p and q. Which is the correct one? Or both are correct? I leave this up to you to decide.

7. **Modular Arithmetic**

   (a) Modular Arithmetic 5
   Solution:
   You people are required to draw the tables yourself.
   Additive Inverses:

   i. Additive Inverse of $0 = 0$
   ii. Additive Inverse of $1 = 4$
   iii. Additive Inverse of $2 = 3$
   iv. Additive Inverse of $3 = 2$
   v. Additive Inverse of $4 = 1$

   Multiplicative Inverses:

   i. Multiplicative Inverse of 0 = Doesn't exist
   ii. Multiplicative Inverse of $1 = 1$
   iii. Multiplicative Inverse of $2 = 3$
   iv. Multiplicative Inverse of $3 = 2$
   v. Multiplicative Inverse of $4 = 4$

   (b) Solve the equations.

   i. $5x + 23 \equiv 6 \bmod 47$
   Solution:
   $5x \equiv -17 \bmod 47$ Now you have to calculate the multiplicative inverse of 5 mod 47. Use the extended GCD to do this.

$EGCD(47, 5) = \{1, -2, 19\}$ So 19 is the multiplicative inverse of 5 mod 47. Hence,

$$x \equiv 19 \cdot -17 \bmod 47 = 6 \bmod 47$$

ii. $9x + 80 \equiv 2 \bmod 81$
Solution:
Inverse doesn't exist, and so there's no solution to x.

iii. system of simultaneous equations
Solution:

$$30x + 3(4 + 13x) \equiv 0 \bmod 37$$

$$69x + 12 \equiv 0 \bmod 37$$

$$32x \equiv 12 \bmod 37$$

So, $EGCD(37, 32) = \{1, 13, -15\}$. So -15 is the multiplicative inverse of 32 mod 37. This implies,

$$x \equiv -15 \cdot -12 \bmod 37 \equiv 32 \bmod 37$$

. So y becomes

$$y \equiv 4 + 13 \cdot 32 \bmod 37 \equiv 13 \bmod 37$$

.

(c) $gcd(5688, 2010)$

$$gcd(5688, 2010) = gcd(2010, 1668)$$

$$= gcd(1668, 342)$$

$$= gcd(342, 300)$$

$$= gcd(300, 42)$$

$$= gcd(42, 6)$$

$$= gcd(6, 0)$$

So,

$$gcd(5688, 2010) = 6$$

(d) Same as Q2(b)