CS70–Spring 2013 — Homework 4

Felix He, SID 303308****

March 31, 2024

Collaborators: None

1. Modulo arithmetic practice

1. Euclid's algorithm: Let $x \geq y > 0$, Then $gcd(x, y) = gcd(y, x \, mod \, y)$

$$\begin{aligned}
\text{gcd}(527, 323) &= \text{gcd}(323, 204) \\
&= \text{gcd}(204, 119) \\
&= \text{gcd}(119, 85) \\
&= \text{gcd}(85, 34) \\
&= \text{gcd}(34, 17) \\
&= \text{gcd}(17, 0) \\
&= 17
\end{aligned}$$

2.

```python
# Extended GCD algorithm
def extended_gcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = extended_gcd(b % a, a)
        return (g, x - (b // a) * y, y)
```

$(x, y) = (27, 5)$	(d, a, b) = e-gcd(5,2) = (1, 1, -2)	return (1, -2, 11)
$(x, y) = (5, 2)$	(d, a, b) = e-gcd(2,1) = (1, 0, 1)	return (1, 1, -2)
$(x, y) = (2, 1)$	(d, a, b) = e-gcd(1, 0) = (1, 1, 0)	return (1, 0, 1)
$(x, y) = (1, 0)$		return (1, 1, 0)

So multiplicative inverse of $5 \, (mod \, 27)$ is $11 \, (mod \, 27)$

3.

$$\begin{aligned}
5x + 26 &\equiv 3 \; mod \; 27 \\
5x &\equiv -23 \; mod \; 27 \\
5x &\equiv 4 \; mod \; 27 \quad \textbf{(multiply both sides with } (5(mod 27))^{-1} \equiv \textbf{11 (mod 27))} \\
x &\equiv 44 \; mod \; 27 \\
x &\equiv 17 \; mod \; 27
\end{aligned}$$

4. False.
   As long as $gcd(a, c)\ |b$, there is a solution.
   To solve $ax \equiv b\ mod\ c$, we cab rewrite it as $ax = kc + b$, suppose $gcd(a, c) = m$, then we have $i \cdot m \cdot x = k \cdot j \cdot m + b$, and since $m|b$, we can write it as $ix - kj = d \to x = \frac{d+kj}{i}$. One example is $2x \equiv 4\ mod\ 6$

2. With these results comes great responsibility...

1. according to Fermat's Little Theorem, $a^{p-1} = 1\ mod\ p$, for any prime number p and a. So 2 is prime, 11 is also prime, $2^{(11-1)}\ mod\ 11 = 1$. $2^{2013} = (2^{10})^{201} * 2^3\ mod\ 11 = 8\ mod\ 11$
2. we can first calculate $5^{2013}\ mod\ 10 = 5$, to see how many exponentials are left after many 2^10 got multiplied, then we just need to calculate $2^5\ mod\ 11 = 10$

3. How many bottles of tea and juice?

The question is trying to solve $37a + 43b = 1250$.
First, we can prove solution exists. $gcd(37, 43) = 1$, we know solve for $(x, y) = (7, -6)$ that makes $37x + 43y = 1$
Second, we multiply both sides with 1250 we get $37(7 * 1250) + 43(-6 * 1250) = 1250$, and we know $\forall k \in Z$ we have $37(7 * 1250 - 43k) + 43(-6 * 1250 + 37k) = 1250$. And since there are constraints for buying goods, which is the quantity ≥ 0. Then we want to find k satisfies both below

$$\begin{cases} 870 - 43k > 10 \\ -7800 + 37k \leq 50 \end{cases} \Rightarrow \begin{cases} k \leq 203 \\ k \geq 203 \end{cases}$$

So $k = 203$ is unique for the equation above. Put it back we get $a = 21, b = 11$

Fibonacci numbers

Proof by induction.
Base case: $n = 1$, $gcd(F(4) + F(2), F(3) + F(1)) = gcd(4, 3) = 1$
IH: assume it holds true for $n = k$, which is $gcd(F(k+3) + F(k+1), F(k+2) + F(k)) = 1$
IS: $n = k + 1$

$$\begin{aligned} & gcd(F(k+4) + F(k+2), F(k+3) + F(k+1)) \\ = & gcd(F(k+3) + F(k+1) + F(k+2) + F(k), F(k+3) + F(k+1)) \end{aligned}$$

Above is exactly the form of $gcd(a + b, a)$ where $a = F(k+3) + F(k+1)$, $b = F(k+2) + F(k)$, and we know $b < a$, $(a + b)\ mod\ a = b$ so according to Euclid's algorithm $gcd(a, b) = gcd(b, a\ mod\ b)$, we have $gcd(a + b, a) = gcd(b, a)$. So we have

$$\begin{aligned} & gcd(F(k+3) + F(k+1) + F(k+2) + F(k), F(k+3) + F(k+1)) \\ = & gcd(F(k+3) + F(k+1), F(k+2) + F(k)) \end{aligned}$$

And according to the induction hypothesis, we know $gcd(F(k+3)+F(k+1), F(k+2)+F(k)) = 1$ holds, so $gcd(F(k+3)+F(k+1)+F(k+2)+F(k), F(k+3)+F(k+1)) = 1$, it holds for $n = k+1$.

Check digits: books and credit cards

1. 1. $d_{10} = 2$. We first calculate $\sum_{i=1}^{9} i \cdot d_i = 189$.
   Then we check for d_{10} from 0 to 9, such that $189 + 10 \cdot d_{10} \equiv 0 \ mod\ 11$, and $d_{10} = 2$

2. to solve $189 + 10 \cdot d_{10} \equiv 0 \ mod\ 11$ is
   to solve $10 \cdot d_{10} \equiv -189 \ mod\ 11$.
   And we know $gcd(11, 10) = 1$, the multiplicative inverse of 10 mod 11 is -1. So multiply both sides of the above equation by $-1\ (mod\ 11)$ we get
   $d_{10} \equiv 189 \ mod\ 11$

3. just like part2, since every number from 1 to 10 is co-prime with 11, since $gcd(i, 11) = 1$. Therefore, for $i \in 1, 2, \ldots, 10$, it has a multiplicative inverse mod 11.
   So every for d_i,

   $$d_i = i^{-1} \cdot \sum_{i=1, i\neq j}^{10} i \cdot d_i \ mod\ 11$$

   d_i is determined already. Any change to it would make it failed to satisfy $\sum_{i=1}^{10} i \cdot d_i \equiv 0 \ mod\ 11$.

4. Invalid.
   The original sum S_1 is $\sum_{i=1}^{10} i \cdot d_i \equiv 0 \ mod\ 11$.
   Suppose we switch j and k, and assume $k > j$ then the new sum S_2 is $1 \cdot d_1 + 2 \cdot d_2 + \ldots + j \cdot d_k + \ldots + k \cdot d_j + \ldots$ Suppose we also want $S_2 \equiv 0 \ mod\ 11$, And then we subtract S_1 from S_2 we get

   $$\begin{aligned} S_1 - S_2 &= kd_k + jd_j - jd_k - kd_j \\ &= (k - j)d_k - (k - j)d_j \\ &= (k - j)(d_k - d_j) \\ &\equiv 0 \ mod\ 11 \end{aligned}$$

   If $(k - j)(d_k - d_j) \equiv 0 \ mod\ 11$, it means $(k - j)(d_k - d_j) = 11m$, $\exists m \in \mathbb{Z}$. Since $(k - j) < 11$ and is co-prime with 11, so we need $(d_k - d_j) < 11$. However, $(d_k - d_j) < 11$, which is also co-prime with 11

5. check digit x is calculated by $(10 - s \ mod\ 10) \ mod\ 10$
   $x = (10 - 72 \ mod\ 10) \ mod\ 10 \equiv 8 \ mod\ 10$

6. No. For example, '09' and '90', no matter how you switch, it remains the same. And if two identical digits both at even or odd digits, even they switch, the sum remains the same.

6. OpRSA

1. 37. $N = 247$, $(p - 1)(q - 1) = 216$, $gcd(37, 216) = 1$

2. $(d, a, b) = extended - gcd(216, 37)$, $b = -35\ (mod\ 216) \equiv 181\ (mod\ 216)$, so $d = 181$

3. $E(m) = m^e\ (mod\ N)$

$$\begin{aligned} 102^2 &\equiv 30 \pmod{247} \\ 102^4 \equiv 30^2 &\equiv 159 \pmod{247} \\ 102^8 \equiv 159^2 &\equiv 87 \pmod{247} \\ 102^{16} \equiv 87^2 &\equiv 159 \pmod{247} \\ 102^{32} \equiv 159^2 &\equiv 87 \pmod{247} \end{aligned}$$

   $102^{37} = 102^{32} \cdot 102^4 \cdot 102^1 = 102 \pmod{247}$

4. $D(E(m)) = m^{ed} = 141^{181} \pmod{247} = 141$

5. The system is wrong for the encryted message is the same with the original one. $x^e \equiv x \pmod{247}$. The resaon why is that is $e = 37$ is co-prime with $p-1$ and $q-1$, which is $e \equiv 1 \pmod{p-1}$ and $e \equiv 1 \pmod{q-1}$. So, $e = 1 + j(p-1)$, $e = 1 + k(q-1)$. By Fermat's little theorem we know, for x is co-prime with p and q, we have $x^{e-1} \equiv e^{j(p-1)}\ mod\ p$ and $x^{e-1} \equiv e^{j(q-1)}\ mod\ q$. And By Chinese Remainder Theorem, $x^{(e-1)} \equiv 1\ mod\ pq$, so $x^e \equiv x\ mod\ pq$. So when we choose e, we better choose e that is not multiplicative inverse with $p-1$ and $q-1$ at the same time.

7. Because the Moth just doesn't cut it

It's not hard. Send message m, use RSA method, (N, e) public key, d as the private key, Make $s = m^d$ to send, and the receiver do s^e, if $m' = s^e \equiv m^{de} \equiv m\ mod\ N$, which means $m' = m$. the message is not corrupted. Otherwise, it's corrupted.