Some suggestions

1. LATEX.
2. Don't be shy to ask.
3. My email: lizy5@shanghaitech.edu.cn

Review

1. cardinality
2. cantor's diagonal argument
3. the definition of ccountable
4. multiset and permutation-intro

Exercise

1.$A = \{\varnothing\}$, write $\mathcal{P}(A)$.

2.Proof or disproof: $|\{(x, y) : x, y \in \mathbb{R}, x^2 + y^2 < 1\}| = |\mathbb{R}|$.

3.Proof or disproof: $|\{S : S \subseteq \mathbb{Z}^+, |S| < \infty\}| = |\mathbb{Z}|$.

Answer

1.$\{\varnothing, \{\varnothing\}\}$.

2.$|\{(x,y) : x, y \in \mathbb{R}, x^2 + y^2 < 1\}| = |(\rho, \theta) : \rho \in [0,1), \theta \in [0, 2\pi)|$

Define $f : \{(\rho, \theta) : \rho \in [0,1), \theta \in [0, 2\pi)\} \to [0,1)$.

$\rho \in [0,1) = 0.a_1a_2a_3\cdots$, $\dfrac{\theta}{2\pi} \in [0,1) = 0.b_1b_2b_3\cdots$

$f((\rho,\theta)) = 0.a_1b_1a_2b_2a_3b_3\cdots \in [0,1)$ who has the same cardinality with $|\mathbb{R}|$.

3.

0	**0**	$\varnothing$
1	1	{1}
2	10	{2}
3	11	{1,2}
4	100	{3}
5	101	{1,3}
6	110	{2,3}
7	111	{1,2,3}
8	1000	{4}
...	...	...

1. (15 points) Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$, and let $q = \lfloor a/b \rfloor$. Show that $\ell(a) - \ell(b) - 1 \leq \ell(q) \leq \ell(a) - \ell(b) + 1$, where $\ell(x)$ is the length of the binary representation of an integer x.

Q1 这道题大家基本上都能做出来，但细节问题比较多。首先，正整数二进制长度的范围

$$\forall x \in \mathbb{N}^*, 2^{l(x)-1} \leq x < 2^{l(x)}, l(x) = \lfloor \log_2 x \rfloor + 1$$

1.

$$2^{l(a)-1} \leq a < 2^{l(a)}, 2^{l(b)-1} \leq b < 2^{l(b)}$$

$$2^{l(a)-l(b)-1} < \frac{a}{b} < 2^{l(a)-l(b)+1}$$

讨论 l(a)-l(b)是否为 0，因为左边可能不是整数

$$2^{l(a)-l(b)-1} \leq \lfloor \frac{a}{b} \rfloor \leq 2^{l(a)-l(b)+1} - 1$$

$$l(a) - l(b) - 1 \leq l(q) \leq l(a) - l(b) + 1$$

2.用地板函数和对数函数的一些性质进行不等式的推导，主要涉及以下式子

$$\lfloor A + B \rfloor \geq \lfloor A \rfloor + \lfloor B \rfloor$$

$$\lfloor A \rfloor - \lfloor B \rfloor - 1 \leq \lfloor A - B \rfloor \leq \lfloor A \rfloor - \lfloor B \rfloor$$

$$\lfloor \log_2(\frac{b}{a}) \rfloor = \lfloor \log_2(\lfloor \frac{b}{a} \rfloor) \rfloor$$

部分同学不等式推导有误

2. (25 points) Implement EEA (Extended Euclidean Algorithm).

By the method introduced in lec6, we have the code:

```
def EEA(a,b):
    s0 = 1; t0 = 0; s1 = 0; t1 = 1
    while a%b !=  0:
        q = a//b
        s2 = s0-q*s1; t2 = t0-q*t1
        s0,t0 = s1,t1; s1,t1 = s2,t2
        a,b = b,a%b
    return s1,t1
```

Taking a and b given in the problem into the fuction, we will have the result:

s=52693465174047597579174064083061206575761398656935114430811243560695066306956
23770063846774138034451326098362590654519415480012670786924252819925030347117 15
36207597896008405650134889458156325490296036336342644796958477425288398387518 17
8265890700656305714837368523496597321973212197144244237647291270529201589

t=-49224356025570205752640369113197589784192495362440084201087757193437212741118
96002459291667895080234292453411578954324261793651077186663625890948400350842 51
28530601681164598597924839372243612858504002463817184486904388029971268441911 21
9848844590762141055813365169533361189741247565502362579257453658280613873

$*Note$: Some students confused s and t.

$i.e.$ using the correct value of s and t here, they get $at + bs = \gcd(a, b)$, which is wrong.

3. (25 points) Implement the Square-and-Multiply algorithm.

```python
def SAM(a,e,n):
    result = 1
    while e > 0:
        if e & 1:
            result = result * a % n
        a = (a * a) % n
        e = e >> 1
    return result
```

Figure 1: reference code

Square: 7pts; Multiply: 7pts; practice in code: 10pts

Result: (1pts)

1948938994538604160707108181724192091954263523362311673846915505520625915922643693886546508713351109692750915684157878314121214348919992352909799653979265473350527870681252083094220999190031833643580240890724902076377092268223725090951395199481472410255314243260591665020918693044381737199432444238061823906089977020969899711341059639979159572739419600905336781673188368650468710718164832109499409767199530541904080512081403155559058709882347747147418230358814131381147208291328747857991048977465984265721979324595417184750317001715144073738047884018946037845800547648474295384881317037454845580697767582076012801834

Common mistakes:

1. As a calculation problem, we want the output.
2. $x_0 = a$ needs to be multiplied into the result according to the value of e0. Some students lack judgment on e0.

Q4 (1) $17x \equiv 11 \mod 23$

$d = \gcd(17, 23) = 1$ —— 2'

$t = (\frac{a}{d})^{-1} \mod (\frac{n}{d})$

$= (17)^{-1} \mod 23$ —— 4'

$= 19 \mod 23$ —— 7'

$x \equiv (\frac{b}{d})\, t \mod (\frac{n}{d})$

$\equiv 11 \times 19 \mod 23$ —— 9'

$\equiv 2 \mod 23$ —— 10'

(2) $55x \equiv 35 \mod 75$

$d = \gcd(55, 75) = 5$ — 2'

$t = (\frac{a}{d})^{-1} \mod (\frac{n}{d})$

$= (11)^{-1} \mod 15$ —— 4'

$= 11 \mod 15$ —— 7'

$x \equiv (\frac{b}{d}) \cdot t \mod (\frac{n}{d})$

$\equiv 7 \times 11 \mod 15$ —— 9'

$\equiv 2 \mod 15$ —— 10'

Note: (1) 求逆过程可以由 EEA 得到，过程不作要求.

(2) 第二问结果应当为模 15，而非 75 (-3)，更有甚者 $75 \div 5 = 25$

(3) 最后结过应化简，即 $x \equiv a \mod n$ $\quad 0 \leq a < n$ (-1)

Q5 Summary

chenzl

Solution (standard & most common):

Yes, Eve can learn the value of m.
According to the process of RSA, we have:

$$c_1 = m^{e1} \ mod \ N$$

$$c_2 = m^{e2} \ mod \ N$$

We know that: $gcd(e_1, e_2) = 1$
By the Bezout's theorem:

$$\exists \ s, t \in \ \mathbb{Z}, s.t. \ e_1 * s + e_2 * t = 1$$

Where s,t can be found by EEA.

$$\begin{aligned} c_1^s * c_2^t \ mod \ N &= (m^{e1} \ mod \ N)^s * (m^{e2} \ mod \ N)^t \\ &= (m^{e1*s} * m^{e2*t}) \ mod \ N \\ &= m^{e1*s+e2*t} \ mod \ N \end{aligned}$$

$$\because \ e_1 * s + e_2 * t = 1$$

$$\therefore \ c_1^s * c_2^t \ mod \ N \ = \ m \ mod \ N$$

$$\therefore \ c_1^s * c_2^t \equiv m \ mod \ N$$

ax≡b

Proved.

常见扣分点

1. $$\because gcd(e_1, e_@) = 1$$ $$\therefore \exists s, t \in \mathbb{Z}, s.t. \ e_1 * s + e_2 * t = 1$$

   这一步没写s，t在整数集内扣1分。

2. s, t可知性，即s，t可以通过EEA求得或s，t可以计算得到确切值。

   这一句没写扣1分。3

. 未写明

$$c_1 = m^{e_1} \ mod \ N$$
$$c_2 = m^{e_2} \ mod \ N$$
$$\Longrightarrow \ m = c_1^s * c_2^t \ mod \ N$$

   的关系推导的扣5分。4

. 书写规范：

$$c_1 = m^{e_1} \ mod \ N$$
写成 $c_1 = m^{e_1} \ \% \ N$

   的扣2-3分。

5. 答案正确，但过程过于简洁或缺乏要点的扣5-9分。6
. 答案正确，但几乎无过程的扣13分。
7. 答案错误，扣13-15分。
8. 未写答案的扣15分。