Homework 4

(1) In the lecture, we have established that to compute $\gcd(a,b)$, $a \geq b$ using Euclidean algorithm requires $O(\log b)$ steps of divisions.

Each division step leads to a remainder:

$$a = bq + r_1 \qquad 0 \leq r_1 < b$$
$$b = r_1 q_1 + r_2 \qquad 0 \leq r_2 < r_1$$
$$r_1 = r_2 q_2 + r_3 \qquad 0 \leq r_3 < r_2$$
$$\vdots$$
$$r_k = r_{k+1} q_{k+1} + r_{k+2}, \qquad r_{k+2} = 0$$

For example: $\gcd(27, 16)$

$r_1 = 11$, $r_2 = 5$, $r_3 = 1$, $r_4 = 0$

After 4 steps, the algorithm terminates.

$\log b = \log 16 = 4$.

For each of the following

sors.

(a) $\gcd(291, 252)$.

(b) $\gcd(16261, 85652)$.

(i) compute the list of remainders (decreasing order till 0)

(ii) Verify that the length of remainders is $O(\log b)$

(iii) Verify that $r_{i+2} \leq \frac{r_i}{2}$ for all i.

(2)

1.25. Let N, g, and A be positive integers (note that N need not be prime). Prove that the following algorithm, which is a low-storage variant of the square-and-multiply algorithm described in Sect. 1.3.2, returns the value $g^A \pmod N$. (In Step 4 we use the notation $\lfloor x \rfloor$ to denote the greatest integer function, i.e., round x down to the nearest integer.)

	Input. Positive integers N, g, and A.
1.	Set $a = g$ and $b = 1$.
2.	Loop while $A > 0$.
	3. If $A \equiv 1 \pmod 2$, set $b = b \cdot a \pmod N$.
	4. Set $a = a^2 \pmod N$ and $A = \lfloor A/2 \rfloor$.
	5. If $A > 0$, continue with loop at Step **2**.
6.	Return the number b, which equals $g^A \pmod N$.

(3) Compute the following $g^x \bmod n$

(a) $17^{183} \pmod{256}$.
(b) $2^{477} \pmod{1000}$.

For each of them, identify the number of multiplications needed using square and multiplication method.

(4) Diffie-Hellman key exchange

Public parameter creation	
A trusted party chooses and publishes a (large) prime p and an integer g having large prime order in $\mathbb{F}_p^*$.	
Private computations	
Alice	**Bob**
Choose a secret integer a.	Choose a secret integer b.
Compute $A \equiv g^a \pmod{p}$.	Compute $B \equiv g^b \pmod{p}$.
Public exchange of values	
Alice sends A to Bob $\longrightarrow$	A
B	$\longleftarrow$ Bob sends B to Alice
Further private computations	
Alice	**Bob**
Compute the number $B^a \pmod{p}$.	Compute the number $A^b \pmod{p}$.
The shared secret value is $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod{p}$.	

Table 2.2: Diffie–Hellman key exchange

Let $p = 941$, $g = 627$.

Alice secret key is $a = 347$

Bob secret key is $b = 781$.

a) Compute A, B, and the number $B^a \bmod p$,

b) $A^b \bmod p$.

Verify that the last two values are equal.

c) What are the values Eve can observe?

d) From these values, what Eve needs to solve to get the shared secret value?