

# CSCI 303 Homework 6

## Problem 1 (31.1-1):

Prove that there are infinitely many primes.

### Solution 1:

Assume that there are only finitely many primes,  $p_1, p_2, \dots, p_k$ . Let

$$n = 1 + \prod_{i=1}^k p_i$$

Then for all  $i \in \{1, 2, \dots, k\}$ , if you divide  $n$  by  $p_i$  the remainder is 1. By the fundamental theorem of arithmetic, all numbers can be written as a product of prime factors. Since none of the primes divide  $n$ , it cannot be the product of prime factors, and we have a contradiction. Therefore our assumption that there are only finitely many primes must be false, so there are infinitely many primes.

## Problem 2 (31.1-7):

For any integer  $k > 0$ , we say that an integer  $n$  is a *kth power* if there exists an integer  $a$  such that  $a^k = n$ . We say that  $n > 1$  is a *nontrivial power* if it is a *kth power* for some integer  $k > 1$ . Show how to determine if a given  $\beta$ -bit integer  $n$  is a nontrivial power in time polynomial in  $\beta$ .

### Solution 2:

Given an  $n$  of  $\beta$  bits, we wish to check whether there exist integers  $a$  and  $k$  such that  $a^k = n$ . Note that  $a \geq 2$  because  $1^k = 1$  for all  $k$ , and  $n$  must be greater than 1 to be a nontrivial power. This implies that  $k$  is at most  $\lfloor \lg n \rfloor$ , because  $a^{\lfloor \lg n \rfloor + 1} > n$  for all  $a \geq 2$ . To determine if  $n$  is a nontrivial power, all we need to do is check whether any of  $n^{1/2}, n^{1/3}, \dots, n^{1/\lfloor \lg n \rfloor}$  are integers. Checking whether the  $m$ th root of  $n$  is an integer can be done in time polynomial in  $\beta$ , and we need to check at most  $\beta$  roots (since  $\lfloor \lg n \rfloor \leq \beta$ ), so determining whether  $n$  is a nontrivial power can be done in time polynomial in  $\beta$ .

## Problem 3 (Derived from 31.2-2):

Use the extended-Euclid's algorithm to compute  $\gcd(899, 493)$  and numbers  $x$  and  $y$  such that  $899x + 493y = \gcd(899, 493)$ . Show your work.

### Solution 3:

$$\text{(eq 1)} \quad 899 = (1) \cdot 899 + (0) \cdot 493$$

$$\text{(eq 2)} \quad 493 = (0) \cdot 899 + (1) \cdot 493$$

$$\text{(eq 3)} \quad 406 = (1) \cdot 899 + (-1) \cdot 493 = \text{(eq 1)} - 1 \cdot \text{(eq 2)} \quad \left(\text{since } \left\lfloor \frac{899}{493} \right\rfloor = 1\right)$$

$$\text{(eq 4)} \quad 87 = (-1) \cdot 899 + (2) \cdot 493 = \text{(eq 2)} - 1 \cdot \text{(eq 3)} \quad \left(\text{since } \left\lfloor \frac{493}{406} \right\rfloor = 1\right)$$

$$\text{(eq 5)} \quad 58 = (5) \cdot 899 + (-9) \cdot 493 = \text{(eq 3)} - 4 \cdot \text{(eq 4)} \quad \left(\text{since } \left\lfloor \frac{406}{87} \right\rfloor = 4\right)$$

$$\text{(eq 6)} \quad 29 = (-6) \cdot 899 + (11) \cdot 493 = \text{(eq 4)} - 1 \cdot \text{(eq 5)} \quad \left(\text{since } \left\lfloor \frac{87}{58} \right\rfloor = 1\right)$$

Finally, we see that  $58 = 2 \cdot 29$ , so  $\gcd(899, 493) = 29$ , and  $29 = (-6) \cdot 899 + (11) \cdot 493$ .

## Problem 4 (Not in book):

Your RSA private key is  $\langle 7, 33 \rangle$ . Digitally sign the message  $M = 9$ . Show your work.

**Solution 4:**

To digitally sign the message, we need to compute  $9^7 \pmod{33}$ .

$$\begin{aligned} 9^7 &= 9 \cdot 9^2 \cdot 9^4 \\ &= 9 \cdot 81 \cdot 81^2 \end{aligned}$$

Here, we need to compute  $81 \pmod{33}$ , and we find that  $81 = (2)33 + 15$ , so  $81 \equiv 15 \pmod{33}$ .

$$\begin{aligned} 9^7 &\equiv 9 \cdot 15 \cdot 15^2 \pmod{33} \\ &\equiv 9 \cdot 15 \cdot 225 \pmod{33} \end{aligned}$$

Next, we need to compute  $225 \pmod{33}$ , and we find that  $225 = (6)33 + 27$ , so  $225 \equiv 27 \pmod{33}$ .

$$\begin{aligned} 9^7 &\equiv 9 \cdot 15 \cdot 27 \pmod{33} \\ &\equiv 135 \cdot 27 \pmod{33} \end{aligned}$$

Next, we need to compute  $135 \pmod{33}$ , and we find that  $135 = (4)33 + 3$ , so  $135 \equiv 3 \pmod{33}$ .

$$\begin{aligned} 9^7 &\equiv 3 \cdot 27 \pmod{33} \\ &\equiv 81 \pmod{33} \\ &\equiv 15 \pmod{33} \end{aligned}$$

Because we found  $81 \equiv 15 \pmod{33}$  earlier.

Therefore, the digital signature of the message  $M = 9$  is  $Sig = 15$ .

**Problem 5 (31.7-1):**

Consider an RSA key set with  $p = 11$ ,  $q = 29$ ,  $n = 319$ , and  $e = 3$ . What value of  $d$  should be used in the secret key? What is the encryption of the message  $M = 100$ ? Show your work.

**Solution 5:**

$$\begin{array}{ll} p = 11 & q = 29 \\ n = p \cdot q & \phi(n) = (p - 1) \cdot (q - 1) \\ = 319 & = 10 \cdot 28 \\ & = 280 \\ e = 3 & \end{array}$$

We need to compute  $d$ . To do so, we use the extended-Euclid's algorithm with inputs 280 and 3.

$$\begin{aligned} 280 &= (1)280 + (0)3 \\ 3 &= (0)280 + (1)3 \\ 1 &= (1)280 + (-93)3 \end{aligned}$$

So  $d = -93 + 280 = 187$ . Let's check it.

$$\begin{aligned}3(187) &= 561 \\561 &\equiv 1 \pmod{280}\end{aligned}$$

The secret key is  $\langle 187, 319 \rangle$ .

Now we wish to encrypt  $M = 100$  using the public key  $\langle 3, 319 \rangle$ . We need to find  $100^3 \pmod{319}$ .

$$\begin{aligned}100^3 &= 100 \cdot 100^2 \\&= 100 \cdot 10\,000\end{aligned}$$

We need to compute  $10\,000 \pmod{319}$ , and we find that  $10\,000 = (31)319 + 111$ , so  $10\,000 \equiv 111 \pmod{319}$ .

$$\begin{aligned}100^3 &\equiv 100 \cdot 111 \pmod{319} \\&\equiv 11\,100 \pmod{319}\end{aligned}$$

Similarly, we find that  $11\,100 = (34)319 + 254$ , so  $11\,100 \equiv 254 \pmod{319}$ .

$$100^3 \equiv 254 \pmod{319}$$

So the cyphertext is  $C = 254$ .