

CSCI303 Fall 2006 Homework 8 Solutions

31.1-1) last updated fall 2006, Yuriy Brun, ybrun@usc.edu

Assume there is a finite number of primes. Let p_1, p_2, \dots, p_n be the sequence of all primes, in order. Consider the number $x = 1 + \prod_{i=1}^n p_i$. It is clear that $x - 1$ divides every prime, thus for every prime, when x is divided by that prime, the remainder is 1. Therefore, x does not divide any of the primes. By the unique factorization theorem, x can be expressed as a product of primes. Therefore, x itself must be prime. But x is larger than p_n . # Contradiction. Therefore there is no largest prime, and therefore there is an infinite number of primes.

31.1-7) last updated fall 2006, Yuriy Brun, ybrun@usc.edu

Given an n of β bits we wish to check if there exists an $a > 0$, and a $k > 1$ such that $a^k = n$. In order for n to be a nontrivial power, some integer root of n must be an integer. So compute the set $A = \{\sqrt[n]{n}, \sqrt[3]{n}, \sqrt[4]{n}, \dots, \sqrt[\lceil \lg n \rceil]{n}\}$. n is a nontrivial power iff there exists an integer element of A . A is of size β , and we can find the i^{th} root of n in $\theta(\beta)$ steps, so this algorithm runs in time polynomial in β .

31.2-2) last updated fall 2006, Yuriy Brun, ybrun@usc.edu

Execution of the algorithm:

| a | b | a/b | d | x | Y |
|-----|-----|-----|----|----|----|
| 899 | 493 | 1 | 29 | -6 | 11 |
| 493 | 406 | 1 | 29 | 5 | -6 |
| 406 | 87 | 4 | 29 | -1 | 5 |
| 87 | 58 | 1 | 29 | 1 | -1 |
| 58 | 29 | 2 | 29 | 0 | 1 |
| 29 | 0 | - | 29 | 1 | 0 |

$d = 29, x = -6, y = 11.$

31.6-1) last updated fall 2006, Yuriy Brun, ybrun@usc.edu

| i | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|-----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|-----------|
| $1^i \bmod 11$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $2^i \bmod 11$ | 1 | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |
| $3^i \bmod 11$ | 1 | 3 | 9 | 5 | 4 | 1 | 3 | 9 | 5 | 4 | 1 |
| $4^i \bmod 11$ | 1 | 4 | 5 | 9 | 3 | 1 | 4 | 5 | 9 | 3 | 1 |
| $5^i \bmod 11$ | 1 | 5 | 3 | 4 | 9 | 1 | 5 | 3 | 4 | 9 | 1 |
| $6^i \bmod 11$ | 1 | 6 | 3 | 7 | 9 | 10 | 5 | 8 | 4 | 2 | 1 |
| $7^i \bmod 11$ | 1 | 7 | 5 | 2 | 3 | 10 | 4 | 6 | 9 | 8 | 1 |
| $8^i \bmod 11$ | 1 | 8 | 9 | 6 | 4 | 10 | 3 | 2 | 5 | 7 | 1 |
| $9^i \bmod 11$ | 1 | 9 | 4 | 3 | 5 | 1 | 9 | 4 | 3 | 5 | 1 |
| $10^i \bmod 11$ | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 |

| | | | | | | | | | | |
|---------------------------|---|----|---|---|---|----|----|----|---|----|
| $x \in \mathbb{Z}_{11}^*$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Order | 1 | 10 | 5 | 5 | 5 | 10 | 10 | 10 | 5 | 2 |

Smallest primitive root $g = 2$.

| | | | | | | | | | | |
|---------------------------|---|---|---|---|---|---|---|---|---|----|
| $x \in \mathbb{Z}_{11}^*$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $\text{ind}_{11,g}(x)$ | 0 | 1 | 8 | 2 | 4 | 9 | 7 | 3 | 6 | 5 |

31.7-1) last updated fall 2006, Yuriy Brun, ybrun@usc.edu

$p = 11, q = 29$

$n = 319$

$\phi(n) = 10(28) = 280$

$e = 3$

We need to compute d . We run extended Euler's algorithm on 280, 3

$$280 = (1) 280 + (0) 3$$

$$3 = (0) 280 + (1) 3$$

$$1 = (1) 280 + (-93) 3$$

So $d = -93 + 280 = 187$. Let's check it. $3(187) \bmod 280 = 561 \bmod 280 = 1$.

So the secret key is $\langle 187, 319 \rangle$.

Now we wish to encrypt 100 using the public key $\langle 3, 319 \rangle$

So we wish to find $100^3 \bmod 319$.

$$100 \bmod 319 = 100$$

$$100^2 \bmod 319 = 10000 \bmod 319 = 111$$

$$100^3 \bmod 319 = 100(111) \bmod 319 = 11100 \bmod 319 = 254$$

So $c = 254$.