MATH 75: Cryptography	Spring 2022

PSET 7 — May 24, 2022

Prof. Asher Auel	*Student: Amittai Siavava*

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***The Code Book*** by **Simon Singh**.
(b) ***Cryptography*** by **Simon Rubinsen-Salzedo**

Problems

1. For the following integers either provide a witness for the compositeness of n or conclude that n is probably prime by providing 5 numbers that are not witnesses. Recall that a witness for the compositeness of n is an integer $a \in \mathbb{Z}$ such that, if we write $n-1 = 2^k u$, where u is odd, then a satisfies $a \not\equiv 0 \pmod{n}$ and $a^u \not\equiv 1 \pmod{n}$ and $a^{2^i u} \not\equiv -1 \pmod{n}$ for all $i = 1, \ldots, k-1$.

(a) $n = 1009$.

$$
\begin{aligned}
2^{1008} &\equiv 1 \pmod{1009} \\
3^{1008} &\equiv 1 \pmod{1009} \\
5^{1008} &\equiv 1 \pmod{1009} \\
7^{1008} &\equiv 1 \pmod{1009} \\
11^{1008} &\equiv 1 \pmod{1009} \\
13^{1008} &\equiv 1 \pmod{1009} \\
17^{1008} &\equiv 1 \pmod{1009}
\end{aligned}
$$

Thus, 1009 is probably prime.
(It actually is! I computedthe values all the way to $1008^{1008} \pmod{1009}$ and they are all equivalent to 1)

(b) $n = 2009$.

$$
\begin{aligned}
2^{2008} &\equiv 1773 \pmod{2009} \\
3^{2008} &\equiv 1313 \pmod{2009} \\
5^{2008} &\equiv 1535 \pmod{2009} \\
7^{2008} &\equiv 980 \pmod{2009} \\
11^{2008} &\equiv 221 \pmod{2009} \\
13^{2008} &\equiv 1240 \pmod{2009} \\
17^{2008} &\equiv 1082 \pmod{2009}
\end{aligned}
$$

Thus, 2009 is NOT prime.

2. Using big-O notation, estimate the number of bit operations required to perform the witness test on $n \in \mathbb{Z}_{>0}$ enough times so that, if n passes all of the tests, it has less than a 10^{-m} chance of being composite.

3. Factor 53477 using the Pollard rho algorithm.

Running pollard's rho algorithm on 53477:

iteration	x	y	$\gcd(\|x-y\|, n)$
1	5	26	1
2	26	30514	1
3	677	15172	1
4	30514	6215	1
5	16150	5526	1
6	15172	4837	53

Thus, two non-trivial factors of 53477 are 53 and $\frac{53477}{53} = 1009$.

4. Fermat and sieving.

(a) Find three nontrivial factors of $n = 99999999999999999999999999999999999919$ by hand.

(b) Let $n = 2^{29} - 1$. Given that

$$\begin{aligned} 258883717^2 &\equiv -2 \cdot 3 \cdot 5 \cdot 29^2 \pmod{n} \\ 301036180^2 &\equiv -3 \cdot 5 \cdot 11 \cdot 79 \pmod{n} \\ 126641959^2 &\equiv 2 \cdot 3^2 \cdot 11 \cdot 79 \pmod{n} \end{aligned}$$

discover a factor of n.

5. Discrete logarithms.

(a) Let $p = 101$. Compute $\log_2 11$ (using complete enumeration by hand).

$$2^{-1} \pmod{101} = 51$$

(1) $$11$$

$$\Downarrow$$

(2) $$\frac{11}{2} \equiv 11 \cdot 51 = 561 \equiv 56 \pmod{101}$$

(3) $$\frac{56}{2} = 28 \pmod{101}$$

(4) $$\frac{28}{2} = 14 \pmod{101}$$

(5) $$\frac{14}{2} = 7 \pmod{101}$$

(6) $$\frac{7}{2} \equiv 7 \cdot 51 = 357 \equiv 54 \pmod{101}$$

(7) $$\frac{54}{2} = 27 \pmod{101}$$

(8) $$\frac{27}{2} \equiv 27 \cdot 51 = 1377 \equiv 64 \pmod{101}$$

(9) $$\frac{64}{2} = 32 \pmod{101}$$

(10) $$\frac{32}{2} = 16 \pmod{101}$$

(11) $$\frac{16}{2} = 8 \pmod{101}$$

(12) $$\frac{8}{2} = 4 \pmod{101}$$

(13) $$\frac{4}{2} = 2 \pmod{101}$$

Thus, $\log_2 11 = 561 \pmod{101}$.

(b) Let $p = 27781703927$ and $g = 5$. Suppose Alice and Bob engage in a Diffie-Hellman key exhange; Alice chooses the secret key $a = 1002883876$ and Bob chooses $b = 21790753397$. Describe the key exchange: what do Alice and Bob exchange, and what is their common (secret) key? *[You may want to use a computer!]*

(c) Let $p = 1021$. Compute $\log_{10} 228$ using the baby step-giant step algorithm. Show the output of, and explain all steps in, your computation.

$$p = 1021$$
$$h = 228$$
$$g = 10$$
$$m = \lceil \sqrt{p} \rceil = 32$$

babysteps $= [h, hg, hg^2, hg^3, \ldots, hg^{m-1}]$
giantsteps $= [g^m, g^{2m}, g^{3m}, \ldots, g^{m^2}]$
Common: $hg^{31} \equiv 921 \equiv g^{16m} \pmod{1021}$

Thus:

$$hg^{31} = g^{16m}$$
$$h = \frac{g^{16m}}{g^{31}} = g^{16m-31}$$
$$\log h = (16m - 31) \cdot \log g$$
$$\log_g h = 16m - 31$$

Thus, $\log_{10} 228 \pmod{1021} = 16 \cdot 32 - 31 = 481$
Which we can confirm by computing $10^{481} \pmod{1021}$, which is (and should be) equivalent to 228

(d) Let $p = 1801$. Compute $\log_{11} 249$ using the Pohlig–Hellman algorithm. Show the output of, and explain all steps in, your computation. You'll want to remind yourself of how to solve systems of congruence equations using Sunzi's theorem: To find $x \in \mathbb{Z}$ satisfying $x \equiv a_i \pmod{n_i}$ for $i = 1, \ldots, k$, first define integers $N_i = \prod_{j \neq i} n_i$ and $M_i \equiv N_i^{-1} \pmod{n_i}$ for all $i = 1, \ldots, k$, and then $x = \sum_{i=1}^{k} a_i N_i M_i$ works.

Let $x = \log_{11} 249 \pmod{1801}$.
Then, $11^x \equiv 249 \pmod{1801}$.

$$p = 1801 \text{ (This is a prime number)}$$
$$\phi(p) = p - 1 = 1800$$
$$\phi(p) = 2^3 \cdot 3^2 \cdot 5^2$$
$$a = \{7, 7, 6\}$$
$$N = \{\ 3^2 \cdot 5^2, 2^3 \cdot 5^2, 2^3 \cdot 3^2\} = \{225, 200, 72\}$$
$$M = \{1, 5, 8\}$$
$$x = \sum_{i=1}^{k} a_i N_i M_i$$
$$x = 7 \cdot 225 + 7 \cdot 200 \cdot 5 + 6 \cdot 72 \cdot 8$$
$$x = 12031$$
$$x \equiv 1231 \pmod{1800}$$

Thus, $\log_{11} 249 \pmod{1801} = 1231$.