Math 134 Homework 6

Nigel Tucker

May 12, 2016

Chapter 6, Exercise 12

You are trying to factor $n = 642401$. Suppose you discover that $516107^2 \equiv 7 \pmod{n}$ and that $187722^2 \equiv 2^2 \cdot 7 \pmod{n}$. Use this information to factor n.

Using the given information we have that $516107^2 \cdot 187722^2 \equiv 7 \cdot 2^2 \cdot 7 \equiv (7 \cdot 2)^2 \pmod{n}$
Now we use the Euclidean Algorithm to compute the greatest common divisor of 642401 and $(516107 \cdot 187722) - (2 \cdot 7) = 96884638240$
$\Rightarrow 96884638240 = 150816 \cdot 642401 + 289024$
$\Rightarrow 642401 = 2 \cdot 289024 + 64353$
$\Rightarrow 289024 = 4 \cdot 64353 + 31612$
$\Rightarrow 64353 = 2 \cdot 31612 + 1129$
$\Rightarrow 31612 = 28 \cdot 1129 + 0$
$\Rightarrow (96884638240, 642401) = 1129$
Now we have found one of our factors of 642401
$\therefore 642401 = 1129 \cdot 569$

Chapter 6, Exercise 13

$880525^2 \equiv 2$, $2057202^2 \equiv 3$, $648581^2 \equiv 6$, $668676^2 \equiv 77 \pmod{2288233}$. How would you use this information to factor 2288233? Explain what the steps you would do, but do not perform the numerical calculations.

We notice that if we multiply the first three congruences together, then the right side is a perfect square. $(880525 \cdot 2057202 \cdot 648581)^2 \equiv 2 \cdot 3 \cdot 6 \equiv (2 \cdot 3)^2 \equiv 6^2 \pmod{2288233}$
The next step of this process is making sure that the left side of the equation is not equal to ± 6 because if it is, then this process will not help us in factoring n.
Once we have ensured that our congruence adheres to the condition above we can find our factor by simply calculating the greatest common divisor of the given n and the $RHS - LHS$ of the equation above, that is compute $gcd((880525 \cdot 2057202 \cdot 648581 - 6), 2288233)$ and this gcd will be the one of the factors we're looking for.
The other factor can be easily found by dividing n by the found gcd.

Chapter 6, Exercise 14

Suppose you have two distinct large primes p and q. Explain how you can find an $x \in \mathbb{Z}$ for which $x^2 \equiv 49 \pmod{pq}$, $x \not\equiv \pm 7 \pmod{pq}$.

If you have two known distinct large primes p and q, in order to find an x for which $x^2 \equiv 49 \pmod{pq}$, but $x \not\equiv \pm 7 \pmod{pq}$ we use the Chinese Remainder Theorem
That is we solve the congruences $x \equiv 7 \pmod{p}$ and $x \equiv -7 \pmod{q}$ (or vice versa with p and q)
$\Rightarrow x^2 \equiv 49 \pmod{p}$ and $\pmod{q}$
$\Rightarrow x^2 \equiv 49 \pmod{pq}$
However $x \not\equiv \pm 7 \pmod{pq}$

Chapter 6, Exercise 23

Your opponent uses RSA with $n = pq$ and encryption exponent e and encrypts message m. This yields the cipher text $c \equiv m^e \pmod{n}$. A spy tells you that, for this message, $m^{12345} \equiv 1 \pmod{n}$. Describe how to determine m. Note that you do not know $p,\ q,\ \varphi(n)$, or the secret decryption exponent d. However, you should find a decryption exponent that works for this particular ciphertext. Moreover explain carefully why your decryption works. For simplicity, assume $\gcd(12345, e) = 1$.

With the spy's leaked information we know that $m^{12345} \equiv 1 \pmod{n}$
We are assuming that $\gcd(12345, e) = 1$, so we can use the Euclidean algorithm to calculate an inverse of e modulo 12345, which we denote d'. Then $ed' = 12345k + 1$ for some integer k. Thus $(m^e)^{d'} \equiv m^{12345k+1} \equiv m^{12345k} \cdot m \equiv 1^k \cdot m \equiv m \pmod{n}$.
This gives us the desired message m.

Chapter 6, Exercise 28

Let s be the smallest integer greater than the square root of n and let $f(x) = (x + s)^2 - n$. Let the factor base B consist of the primes up to some bound B. We want to find squares that are congruent mod n to a product of primes in B. One way to do this is to find values of $f(x)$ that are products of primes in B. We'll search over a range $0 \le x \le A$, for some A.

(a) Suppose $0 \le x < (\sqrt{2} - 1)\sqrt{n} - 1$. Show that $0 \le f(x) < n$, so $f(x) \pmod{n}$ is simply $f(x)$. Henceforth, we'll assume that $A < (\sqrt{2}-1)\sqrt{n}-1$, so the values of x that we consider have $f(x) < n$.

Using the hint given we attempt to show that $x + s < \sqrt{2n}$
Well assuming $0 \le x < (\sqrt{2} - 1)\sqrt{n} - 1$ we have that
$x + s < (\sqrt{2} - 1)\sqrt{n} - 1 + s = \sqrt{2}\sqrt{n} - \sqrt{n} - 1 + \lceil \sqrt{n} \rceil < \sqrt{2n} - \sqrt{n} - 1 + \sqrt{n} + 1 = \sqrt{2n}$
$\Rightarrow x + s < \sqrt{2n}$
$\Rightarrow f(x) = (x + s)^2 - n < (\sqrt{2n})^2 - n = 2n - n = n$
$\Rightarrow f(x) < n$ as we wanted to show
$\Rightarrow f(x) \pmod{n} = f(x)$

(b) Let p be a prime in B. Show that if the exists an integer x with $f(x)$ divisible by p, then n is a square (mod p). This shows that we may discard those primes in B for which n is not a square mod p. Henceforth we will assume that such primes have been discarded.

Assuming $\exists\ x$ for which $p \mid f(x) = (x + s)^2 - n$
$\Rightarrow (x + s)^2 - n = kp$ for some $k \in \mathbb{Z}$
$\Rightarrow (x + s)^2 - kp = n$
Now if reduce (mod p) we have that
$(x + s)^2 - kp \equiv (x + s)^2 \equiv n \pmod{p}$
$\Rightarrow n$ is in fact a square when we reduce (mod p)

(c) Let $p \in B$ be such that n is a square mod p. Show that if p is odd, and $p \nmid n$, then there are exactly two values of x mod p such that $f(x) \equiv 0 \pmod{p}$. Call these values $x_{p,1}$ and $x_{p,2}$.

We know that from part 2 we have that there exists an a such that $n \equiv a^2 \pmod{p}$
And since $p \nmid n$
$\Rightarrow a \not\equiv 0 \pmod{n}$
$\Rightarrow 0 \equiv f(x) = (x+s)^2 - a^2 \equiv ((x+s)+a)((x+s)-a) \pmod{p}$
Now using the fact that p is a prime we know that if $p \mid f(x)$
$\Rightarrow p \mid ((x+s)+a)$ or $p \mid ((x+s)-a)$
$\Rightarrow ((x+s)+a)$ or $((x+s)-a) \equiv 0 \pmod{p}$
$\Rightarrow x \equiv -a-s$ or $a-s \pmod{p}$
Now since p was assumed to be an odd prime and $a \not\equiv 0 \pmod{p}$,
the two solutions $x_{p,1} \equiv -a-s$ and $x_{p,2} \equiv a-s$ are distinct.

(d) For each x with $0 \leq x \leq A$, initialize a register with value $log[f(x)]$. For each prime $p \in B$ subtract $log(p)$ from the registers of those x with $x \equiv x_{p,1}$ or $x_{p,2} \pmod{p}$. Show that if $f(x)$ (with $0 \leq x \leq A$) is a product of distinct primes in B, then the register for x becomes 0 at the end of this process.

Suppose that $f(x)$ is the product of distinct primes in B:
$f(x) = p_1 p_2 ... p_k$, with each $p_i \in B$. By part (c), $p_i \mid f(x)$ implies that $x \equiv x_{p_i,1}$ or $x \equiv x_{p_i,2}$, and hence $\log(p_i)$ will be subtracted from the register for x when we reach the prime p_i. Conversely, if $p \in B$ but p is not one of the p_i, then p does not divide $f(x)$ and hence x is not equivalent to $x_{p,1}$ or $x_{p,2} \pmod{p}$. Therefore nothing will happen to the register of x at the prime p. Therefore, when we pass through all the primes in B, exactly the values $\log(p_i)$ for $i = 1, \ldots, k$ will be subtracted from the register for x. The value of the register for x at the end of the process will therefore be $\log[f(x)] - \log(p_1) - \log(p_2) - ... - \log(p_k) = 0$
$\Rightarrow$ the register for x becomes 0.

(e) Explain why it is likely that if $f(x)$ is a product of (possibly nondistinct) primes in B then the final result for the register for x is small (compared to the register for an x such that $f(x)$ has a prime factor not in B).

If $f(x)$ has a large prime factor p, the our register will be at least $log(p)$ which will also be rather large.
Also we have shown in part 4 that if all of the prime factors of $f(x)$ are both distinct and in B
$\Rightarrow$ the register will be 0
Now for the more general case
We know by constriction that the register will contain the sum of logs of the primes contained in B
$\Rightarrow$ our register will tend to be small
Also since it is much more likely that our $f(x)$ will be divisible by multiple small primes rather than multiple large primes
$\Rightarrow$ with multiplicty of primes we still conclude that our register will tend towards being relatively small

(f) We are checking the integers up to A. If we checked divisibility for each combination, we would have to compute $f(x)$ and then divide by p for each of the A choices for x. However, once we determine the x_{p_1} and x_{p_2}, there are no divisibilities that we need to check; we simply subtract $\log(p)$ from the register for $x = x_{p_1}, x_{p_1} + p, x_{p_1} + 2p, \ldots$ and similarly for x_{p_2}. Thus we do not have to check any divisibilities and we only have to do $2[A/p]$ subtractions. Subtraction is a much faster operation than multiplication and division for a computer to handle, and we are doing far fewer of them! So the method described here is much faster than the brute force method.

Chapter 7, Exercise 1

1. Let $p = 13$. Compute $L_a(3)$.

   It is easy to see that $2^4 = 16 \equiv 3 \pmod{13}$
   $\Rightarrow L_a(3) = 4$

2. Show that $L_2(11) = 7$.

   Using the definition of the discrete log we have that $2^7 = 128 \equiv -2 \equiv 11 \pmod{13}$
   $\Rightarrow L_2(11) = 7$

Chapter 7, Exercise 2

1. Compute $6^5 \pmod{11}$.

   Well using that fact that $6^2 = 36 \equiv 3 \pmod{11}$
   $\Rightarrow (6^2)^2 \equiv 3^2 \equiv 9 \pmod{11}$
   $\Rightarrow (6^2)^2(6) \equiv 9(6) \equiv 54 \equiv 10 \pmod{11}$
   $\therefore 6^5 \equiv -1 \equiv 10 \pmod{11}$

2. Let $p = 11$. Then 2 is a primitive root. Suppose $2^x \equiv 6 \pmod{11}$. Without finding the value of x, determine whether x is even or odd.

   Since 2 is a primitive root $\pmod{11}$
   $\Rightarrow 2^{\frac{\varphi(11)}{2}} = 2^{\frac{10}{2}} = 2^5 \equiv -1 \pmod{11}$
   $\Rightarrow -1 \equiv 6^5 \equiv (2^x)^5 \equiv (2^5)^x \equiv (-1)^x \pmod{11}$
   $\therefore x$ must be odd

Chapter 7, Exercise 3

It can be shown that 5 is a primitive root for the prime 1223. You want to solve the discrete logarithm problem $5^x \equiv 3 \pmod{1223}$. Given that $3^{611} \equiv 1 \pmod{1223}$, determine whether x is even or odd.

Using the fact that 5 is a primitive root we know that
$5^{\frac{\varphi(1223)}{2}} \equiv (-1)^{\frac{1222}{2}} \equiv (-1)^{611} \equiv -1 \pmod{1223}$
We are given that $1 \equiv 3^{611} \pmod{1223}$
Now putting both of these together we have that
$1 \equiv 3^{611} \equiv (5^x)^{611} \equiv (5^{611})^x \equiv (-1)^x \pmod{1223}$
$\therefore x$ must be even

Chapter 7, Exercise 10

In Diffie-Hellman key exchange protocol, Alice and Bob choose a primitive root α for a large prime p. Alice sends $x_1 \equiv \alpha^a \pmod{p}$ to Bob, and Bob sends $x_2 \equiv \alpha^b \pmod{p}$ to Alice. Suppose Eve bribes Bob to tell her the values of b and x_2. However, he neglects to tell her the value of α. Suppose $(b, p-1) = 1$. Show how Eve can determine α from the knowledge of p, x_2 and b.

Since p has been made public, $(b, p-1) = 1$, and Eve has bribed Bob into telling her the values of b and x_2
$\Rightarrow$ all Eve has to do is compute c for which $bc \equiv 1 \pmod{p-1}$
Then compute $(x_2)^c \pmod{p}$ as $(x_2)^c \equiv (\alpha^b)^c \equiv (\alpha)^{bc} \equiv \alpha \pmod{p}$