CS 70 Discrete Mathematics and Probability Theory
Spring 2017 Rao

HW 5

1 Sundry

Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. (In case of homework party, you can also just describe the group.) How did you work on this homework? Working in groups of 3-5 will earn credit for your "Sundry" grade.

Please copy the following statement and sign next to it:

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up. (Signature here)

2 Count and Prove

(a) Over 1000 students walked out of class and marched to protest the war. To count the exact number of students protesting, the chief organizer lined the students up in columns of different length. If the students are arranged in columns of 3, 5, and 7, then 2, 3, and 4 people are left out, respectively. What is the minimum number of students present? Solve it with Chinese Remainder Theorem.

(b) Prove that for $n \geq 1$, if $935 = 5 \times 11 \times 17$ divides $n^{80} - 1$, then 5, 11, and 17 do not divide n.

Solution:

(a) Let the number of students be x. The problem statement allows us to write the system of congruences:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7. \end{aligned} \tag{1}$$

To apply CRT, we first find the multiplicative inverse of 5×7 modulo 3, which is 2. This gives us

$$y_1 = (5 \times 7) \times \left((5 \times 7)^{-1} \pmod 3\right) = 35 \times 2 = 70.$$

Second, we compute the multiplicative inverse of 3×7 modulo 5, which is 1. We have

$$y_2 = (3 \times 7) \times \left((3 \times 7)^{-1} \pmod 5\right) = 21 \times 1 = 21.$$

Finally, the the multiplicative inverse of 3×5 modulo 7 is 1. Thus,

$$y_3 = (3 \times 5) \times \left((3 \times 5)^{-1} \pmod 7\right) = 15 \times 1 = 15.$$

By CRT, we can write down the unique solution x (modulo $105 = 3 \times 5 \times 7$):

$$\begin{aligned} x &= a_1 y_1 + a_2 y_2 + a_3 y_3 \pmod{105} \\ &= 2 \times 70 + 3 \times 21 + 4 \times 15 \pmod{105} \\ &= 263 \pmod{105} \\ &= 53 \pmod{105}. \end{aligned}$$

Now, we have $x = 105k + 53$ for some integer k. The smallest k for $x > 1000$ is 10. Thus, the mininum number of students is $105 \times 10 + 53 = 1103$.

(b) Note that $935 = 5 \times 11 \times 17$. We wish to prove that if $n^{80} \equiv 1 \pmod{935}$ then $5, 11, 17 \nmid n$.

Since $n^{80} \equiv 1 \pmod{935}$, we know that $n^{80} = 935k + 1$ for some integer k. Thus, we know $n^{80} \equiv 1 \pmod 5$, $n^{80} \equiv 1 \pmod{11}$, and $n^{80} \equiv 1 \pmod{17}$.

We will now prove the statement by contradiction. Let us now assume the contrary; i.e., that $n^{80} \equiv 1 \pmod{935}$ and either $5 \mid n$ or $11 \mid n$ or $17 \mid n$. Then we have 3 possible cases:

- If $5 \mid n$ then, $n = 5k$, which implies $n \equiv 0 \pmod 5$, which in turn implies $n^{80} \equiv 0 \pmod 5$,
- If $11 \mid n$ then, $n = 11k$, which implies $n \equiv 0 \pmod{11}$, which in turn implies $n^{80} \equiv 0 \pmod{11}$,
- If $17 \mid n$ then, $n = 17k$, which implies $n \equiv 0 \pmod{17}$, which in turn implies $n^{80} \equiv 0 \pmod{17}$,

which are all false as under the assumptions that $n^{80} \equiv 1 \pmod{935}$, since this implies $n^{80} \equiv 1 \pmod 5$, $n^{80} \equiv 1 \pmod{11}$, and $n^{80} \equiv 1 \pmod{17}$. Thus we have reached a contradiction, and we must have that $5, 11, 17 \nmid n$.

3 RSA Lite

Woody misunderstood how to use RSA. So he selected prime $P = 101$ and encryption exponent $e = 67$, and encrypted his message m to get $35 = m^e \bmod P$. Unfortunately he forgot his original message m and only stored the encrypted value 35. But Carla thinks she can figure out how to recover m from $35 = m^e \bmod P$, with knowledge only of P and e. Is she right? Can you help her figure out the message m? Show all your work.

Solution:

Recall that the security of RSA depended upon the supposed hardness of factoring $N = P \times Q$. However, since $N = P$ in this problem, we can consider it to have been already factored! Indeed, recall that the private key d in RSA is defined to be the multiplicative inverse of e modulo $(P-1)(Q-1)$, because we can then use the following relation to decrypt the message:

$$m^{k(P-1)(Q-1)+1} \equiv m \pmod{N}$$

Note that in our case where $N = P$, an analogous relation immediately holds by Fermat's Little Theorem:

$$m^{k(P-1)+1} \equiv m \pmod{P}$$

Therefore, if we can find d which is the multiplicative inverse of e modulo $P-1$, we can decrypt the message by simply computing $m^{ed} \pmod{P} = 35^d \pmod{P}$. It is easy to see by inspection that $67 \times 3 = 201 \equiv 1 \pmod{100}$, so the desired multiplicative inverse $d = 3$, which means that $m = 353 \pmod{101} = 51 \pmod{101}$.

(Otherwise, one can find the multiplicative inverse by applying Extended Euclid's algorithm to $e = 67$ and $P - 1 = 100$:

$$\begin{aligned}
(c,a,b) &= \text{extended-gcd}(100,67) = (c, b_1, a_1 - \lfloor 100/67 \rfloor b_1) \quad \text{where} \\
(c,a_1,b_1) &= \text{extended-gcd}(67,33) = (c, b_2, a_2 - \lfloor 67/33 \rfloor b_2) \quad \text{where} \\
(c,a_2,b_2) &= \text{extended-gcd}(33,1) = (c, b_3, a_3 - \lfloor 33/1 \rfloor b_3) \quad \text{where} \\
(c,a_3,b_3) &= \text{extended-gcd}(1,0) = (1,1,0)
\end{aligned}$$

Therefore, $(c,a_2,b_2) = (1,0,1)$, $(c,a_1,b_1) = (1,1,-2)$, and $(c,a,b) = (1,-2,3)$ respectively. We can verify that $1 = c = ax + by = -2 \times 100 + 3 \times 67$. Hence, the multiplicative inverse of 67 modulo 100 is 3.)

4 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p,q,r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \bmod N$.

Solution:

$N = pqr$ where p,q,r are all prime. Then, let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N,e) and calculate $d = e^{-1} \bmod (p-1)(q-1)(r-1)$. People who wish to send me a secret, x, send $y = x^e \bmod N$. I decrypt an incoming message, y, by calculating $y^d \bmod N$.

Does this work? We prove that $x^{ed} - x \equiv 0 \bmod N$ and thus $x^{ed} \equiv x \bmod N$. To prove that $x^{ed} - x \equiv 0 \bmod N$, we factor out the x to get $x \cdot (x^{ed-1} - 1) = x \cdot (x^{k(p-1)(q-1)(r-1)+1-1} - 1)$ because $ed \equiv 1 \bmod (p-1)(q-1)(r-1)$. As a reminder, we are considering the number: $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$.

We now argue that this number must be divisible by p, q, and r. Thus it is divisible by N and $x^{ed} - x \equiv 0 \bmod N$.
To prove that it is divisible by p:

- If x is divisible by p, then the entire thing is divisible by p.
- If x is not divisible by p, then that means we can use FLT on the inside to show that $(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \bmod p$. Thus it is divisible by p.

To prove that it is divisible by q:

- If x is divisible by q, then the entire thing is divisible by q.
- If x is not divisible by q, then that means we can use FLT on the inside to show that $(x^{q-1})^{k(p-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \bmod q$. Thus it is divisible by q.

To prove that it is divisible by r:

- If x is divisible by r, then the entire thing is divisible by r.
- If x is not divisible by r, then that means we can use FLT on the inside to show that
$$(x^{r-1})^{k(p-1)(q-1)} - 1 \equiv 1 - 1 \equiv 0 \bmod r.$$
Thus it is divisible by r.

5 Squared RSA

(a) Prove the identity $a^{p(p-1)} \equiv 1 \pmod{p^2}$, where a is relatively prime to p and p is prime.

(b) Now consider the RSA scheme: the public key is $(N = p^2q^2, e)$ for primes p and q, with e relatively prime to $p(p-1)q(q-1)$. The private key is $d = e^{-1} \pmod{p(p-1)q(q-1)}$. Prove that the scheme is correct, i.e. $x^{ed} \equiv x \pmod{N}$. You may assume that x is relatively prime to both p and q.

(c) Continuing the previous part, prove that the scheme is unbreakable, i.e. your scheme is at least as difficult as ordinary RSA.

Solution:

(a) Consider the set S of all numbers between 1 and $p^2 - 1$ (inclusive) which are relatively prime to p. Consider the map $f(x) = ax$, and let T be the image of S, i.e. $T = f(S)$. Since a is relatively prime to p, and therefore relatively prime to p^2, we know that $a^{-1} \pmod{p^2}$ exists, modulo p^2. Since the inverse exists, we know that $f(x)$ has an inverse map, and is therefore a bijection: $|S| = |T|$. To show that $S = T$, it suffices to show that $T \subseteq S$. But if $t \in T$, then $t = as$ for some $s \in S$ with s relatively prime to p^2. Since a is also relatively prime to p^2, then $as = t$ is also relatively prime to p^2. We have shown that $t \in T$ implies $t \in S$, so $T \subseteq S$ (and by the discussion above, $T = S$). Finally, observe that the product of the elements of S is the same as the product of the elements of T, so

$$\prod_{i=1}^{|S|}\{s : s \in S\} = \prod_{i=1}^{|S|}\{t : t \in S\} \pmod{p^2}$$
$$= a^{|S|}\prod_{i=1}^{|S|}\{s : s \in S\} \pmod{p^2}$$

so we can conclude that $a^{|S|} \equiv 1 \pmod{p^2}$. To conclude the argument, we show that $|S| = p(p-1)$. But there are p^2 numbers between 1 and p^2, and if we subtract the p multiples of p, we end up with $|S| = p^2 - p = p(p-1)$.

(b) By the definition of d above, $ed = 1 + kp(p-1)q(q-1)$ for some k. Look at the equation $x^{ed} \equiv x \pmod N$ modulo p^2 first:

$$x^{ed} \equiv x^{1+kp(p-1)q(q-1)} \equiv x \cdot (x^{p(p-1)})^{kq(q-1)} \equiv x \pmod{p^2}$$

where we used the identity above. If we look at the equation modulo q^2, we obtain the same result. Hence, $x^{ed} \equiv x \pmod{p^2q^2}$.

(c) We consider the scheme to be broken if knowing p^2q^2 allows you to deduce $p(p-1)q(q-1)$. (Observe that knowing $p(p-1)q(q-1)$ is enough, because we can compute the private key with this information.) Suppose that the scheme can be broken; we will show how to break ordinary RSA. For an ordinary RSA public key $(N = pq, e)$, square N to get $N^2 = p^2q^2$. By our assumption that the squared RSA scheme can be broken, knowing p^2q^2 allows us to find $p(p-1)q(q-1)$. We can divide this by $N = pq$ to obtain $(p-1)(q-1)$, which breaks the ordinary RSA scheme. This proves that our scheme is at least as difficult as ordinary RSA.

Remark: The first part of the question mirrors the proof of Fermat's Little Theorem. The second and third parts of the question mirror the proof of correctness of RSA.

6 Breaking RSA

(a) Eve is not convinced she needs to factor $N = pq$ in order to break RSA. She argues: "All I need to know is $(p-1)(q-1)$... then I can find d as the inverse of e mod $(p-1)(q-1)$. This should be easier than factoring N." Prove Eve wrong, by showing that if she knows $(p-1)(q-1)$, she can easily factor N (thus showing finding $(p-1)(q-1)$ is at least as hard as factoring N). Assume Eve has a friend Wolfram, who can easily return the roots of polynomials over $\mathbb{R}$ (this is, in fact, easy).

(b) When working with RSA, it is not uncommon to use $e = 3$ in the public key. Suppose that Alice has sent Bob, Carol, and Dorothy the same message indicating the time she is having her birthday party. Eve, who is not invited, wants to decrypt the message and show up to the party. Bob, Carol, and Dorothy have public keys $(N_1, e_1), (N_2, e_2), (N_3, e_3)$ respectively, where

$e_1 = e_2 = e_3 = 3$. Furthermore assume that N_1, N_2, N_3 are all different. Alice has chosen a number $0 \leq x < \min\{N_1, N_2, N_3\}$ which indicates the time her party starts and has encoded it via the three public keys and sent it to her three friends. Eve has been able to obtain the three encoded messages. Prove that Eve can figure out x. First solve the problem when two of N_1, N_2, N_3 have a common factor. Then solve it when no two of them have a common factor. Again, assume Eve is friends with Wolfram as above.

Hint: The concept behind this problem is the Chinese Remainder Theorem: Suppose $n_1, \ldots, n_k$ are positive integers, that are pairwise co-prime. Then, for any given sequence of integers $a_1, \ldots, a_k$, there exists an integer x solving the following system of simultaneous congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Furthermore, all solutions x of the system are congruent modulo the product, $N = n_1 \cdots n_k$. Hence: $x \equiv y \pmod{n_i}$ for $1 \leq i \leq k \Leftrightarrow x \equiv y \pmod{N}$.

Solution:

(a) Let $a = (p-1)(q-1)$. If Eve knows $a = (p-1)(q-1) = pq - (p+q) + 1$, then she knows $p + q = pq - a + 1$ (note that $pq = N$ is known too). In fact, p and q are the two roots of polynomial $f(x) = x^2 - (p+q)x + pq$ because $x^2 - (p+q)x + pq = (x-p)(x-q)$. Since she knows $p+q$ and pq, she can give the polynomial $f(x)$ to Wolfram to find the two roots of $f(x)$, which are exactly p and q.

Alternate Solution: Consider the polynomial $r(x) = (x-p)(x-q)$. Evaluate the polynomial at three special points.

$$\begin{aligned} r(0) &= N \\ r(1) &= (p-1)(q-1) \\ r(N) &= N(p-1)(q-1) \end{aligned}$$

Use polynomial interpolation to find the polynomial that goes through the three points $(0, N)$, $(1, (p-1)(q-1))$, $(N, N(p-1)(q-1))$, and then ask Wolfram for the roots of the polynomial.

(b) Eve first tests the GCD of all pairs of N_1, N_2, N_3. Let $d_1 = \gcd(N_1, N_2)$, $d_2 = \gcd(N_2, N_3)$, and $d_3 = \gcd(N_1, N_3)$. Then there are two cases:

case 1 If one of the d_1, d_2, or d_3 is greater than 1, it must be one of the prime factors p of the two N_i's. The other prime factor q can be recovered by $q = N_i/p$. Therefore, we can factorize one of the N_i's and once we do that, RSA is broken.

case 2 If $d_1 = d_2 = d_3 = 1$, it means all pairs of the N_i's are coprime. Let the three encoded messages be y_1, y_2, y_3. Since the messages are encoded by RSA with public keys $(N_1, 3)$, $(N_2, 3)$, and $(N_3, 3)$, we have:

$$x^3 \equiv y_1 \bmod N_1$$
$$x^3 \equiv y_2 \bmod N_2$$
$$x^3 \equiv y_3 \bmod N_3$$

Since all pairs of N_1, N_2, N_3 are coprime, by using the Chinese Remainder Theorem, we can solve the above system of congruence equations. Let the solution be

$$x^3 \equiv x_0 \bmod N_1 N_2 N_3$$

with $0 \le x_0 < N_1 N_2 N_3$. Since $x < N_1, N_2, N_3$, $x^3 < N_1 N_2 N_3$, and thus $x^3 = x_0$. We can take the cube root of x_0 and recover the original message $x = x_0^{1/3}$. In this problem, the trick is that we were able to convert a problem of finding cube-roots mod a prime (which is hard) into finding cube-roots in the integers (which is easy).

7 Polynomials in Fields

Define the sequence of polynomials by $P_0(x) = x + 12$, $P_1(x) = x^2 - 5x + 5$ and $P_n(x) = xP_{n-2}(x) - P_{n-1}(x)$.
(For instance, $P_2(x) = 17x - 5$ and $P_3(x) = x^3 - 5x^2 - 12x + 5$.)

(a) Show that $P_n(7) \equiv 0 \pmod{19}$ for every $n \in \mathbb{N}$.

(b) Show that, for every prime q, if $P_{2017}(x) \not\equiv 0 \pmod{q}$, then $P_{2017}(x)$ has at most 2017 roots modulo q.

Solution:

(a) Prove by strong induction. Base cases:

$$P_0(7) \equiv 7 + 12 \equiv 19 \equiv 0 \pmod{19}$$
$$P_1(7) \equiv 7^2 - 5 \cdot 7 + 5 \equiv 49 - 35 + 5 \equiv 19 \equiv 0 \pmod{19}$$

Inductive step: Assume $P_n(7) \equiv 0 \pmod{19}$ for every $n \le k$. Then

$$\begin{aligned} P_{k+1}(7) &\equiv xP_{k-1}(7) - P_k(7) \pmod{19} \\ &\equiv x \cdot 0 - 0 \pmod{19} \\ &\equiv 0 \pmod{19}. \end{aligned}$$

Hence, we have $P_n(7) \equiv 0 \pmod{19}$ for all naturnal numbers n.

(b) This question asks to prove that, for all prime numbers q, if $P_{2017}(x)$ is a non-zero polynomial $\pmod{q}$, then $P_{2017}(x)$ has at most 2017 roots $\pmod{q}$.

The proof of Property 1 of polynomials (a polynomial of degree d can have at most d roots) still works in the finite field $\mathrm{GF}(q)$. Therefore we need only show that P_{2017} has degree at most 2017. We prove that $\deg(P_n) \leq n$ for $n > 1$ by strong induction. Base cases:

$$\begin{aligned}
\deg(P_0) &= \deg(x+12) = 1 \\
\deg(P_1) &= \deg(x^2-5x+5) = 2 \\
\deg(P_2) &= \deg(xP_0(x) - P_1(x)) \leq 2 \\
\deg(P_3) &= \deg(xP_1(x) - P_2(x)) \leq 3
\end{aligned}$$

Assuming degree of $P_n \leq n$ for all $2 \leq n \leq k$, then

$$\begin{aligned}
\deg(P_{k+1}(x)) &\leq \max\{\deg(xP_{k-1}(x)), \deg(P_k(x))\} \\
&= \max\{1+\deg(P_{k-1}(x)), \deg(P_k(x))\} \\
&\leq \max\{1+k-1, k\} \\
&\leq k \\
&\leq k+1.
\end{aligned}$$

Thus the proof holds for all $n \geq 2, n \in \mathbb{N}$.