CS 70 Discrete Mathematics and Probability Theory
Summer 2015 Chung-Wei Lin Discussion 3A

1. Basic RSA Operations

Consider an RSA scheme modulus $N = pq$, where p and q are prime numbers larger than 3. In this setting, Alice wants to send a message x to Bob with public key (N, e).

(a) Now suppose that $p = 11$, $q = 17$, and $e = 3$. Find the secret key d used in this scheme.
d must be the multiplicative inverse of 3 (mod 160), so $d = 107$.

(b) Alice wants to send a message $x = 70$ to Bob. What is the encrypted message she sends using the public key?
$x^3 = 42 \pmod{187}$.

2. RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve who is listening to all of their communications notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(e, N_1), \ldots, (e, N_k)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

(a) Suppose Eve sees the public keys $(7, 35)$ and $(7, 77)$ as well as the corresponding transmissions. Note that $\gcd(77, 35) = 7$. Can Eve use this knowledge to break the encryption?
Yes. She can figure out the gcd of the two numbers using the gcd algorithm, and then divide 35 by 7, getting 5. Then she knows that the p and q corresponding to the first transmission are 7 and 5 (7 and 11 for the second transmission), and can break the encryption.

(b) The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(3, 5 \times 23)$, $(3, 11 \times 17)$, and $(3, 29 \times 41)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above.
Since none of the N's have common factors, she cannot find a gcd to divide out of any of the N's. Hence the approach above does not work. (We assume factoring the product of two prime numbers is impossible, or extremely difficult. In real implementation, two very large primes will be used.)

(c) Recall that these public keys imply that $(x < 5 \times 23) \wedge (x < 11 \times 17) \wedge (x < 29 \times 41)$. Let us suppose for this part and the next that the society chose $x = 100$ (though Eve doesn't know!). Is x^3 greater or less than $(5 \times 23)(11 \times 17)(29 \times 41)$?
Less. This can be seen as follows: $(5 \times 23)(11 \times 17)(29 \times 41) > (100)(100)(100) = x^3$.

(d) Imagine that, from the transmissions above, Eve can figure out $x^3 \bmod (5 \times 23)(11 \times 17)(29 \times 41)$. In addition, give her a machine that lets her take cube-roots of integers. Can Eve deduce x?
Yes. Since $x^3 < (5 \times 23)(11 \times 17)(29 \times 41)$, by figuring out $x^3 \bmod (5 \times 23)(11 \times 17)(29 \times 41)$ she figures out x^3. Then she can just take the cube root to get x.

3. Roots

Let's make sure you're comfortable with thinking about roots of polynomials in familiar old $\mathbb{R}$. For all of these questions, take the context to be $\mathbb{R}$:

(a) True or False: if $p(x) = ax^2 + bx + c$ has two positive roots, then $ab < 0$ and $ac > 0$. Argue why or provide a counterexample.

True. $-b/a$ is the sum of the two roots, while c/a is the product of the two roots. These must both be positive, while multiplying them through by the positive value a^2 shows they have the same signs as $-ab$ and ac, respectively.

(b) Suppose $P(x)$ and $Q(x)$ are two different nonzero polynomials with degrees d_1 and d_2 respectively. What can you say about the number of solutions of $P(x) = Q(x)$? How about $P(x) \cdot Q(x) = 0$?

The number of solutions of $P(x) = Q(x)$ is at most $\max(d_1, d_2)$. The number of solutions of $P(x) \cdot Q(x) = 0$ is at most $d_1 + d_2$.

(c) We've given a lot of attention to the fact that a nonzero polynomial of degree d can have at most d roots. Well, I'm sick of it. What I want to know is, what is the *minimal* number of real roots that a nonzero polynomial of degree d can have? How does the answer depend on d?

If d is even, 0 (consider $x^d + 1$); otherwise, 1 (a polynomial of odd degree takes on arbitrarily large positive and negative values, and thus must pass through 0 inbetween them at least once).

(d) Consider the degree 2 polynomial $f(x) = x^2 + ax + b$. Show that, if f has exactly one root, then $a^2 = 4b$.

If there is a root c, then the polynomial is divisible by $x - c$. Therefore it can be written as $(x - c)g(x)$. But $g(x)$ is a degree one polynomial and by looking at coefficients it is obvious that its leading coefficient is 1. Therefore $g(x) = x - d$ for some d. But then d is also a root, which means that $d = c$. So $f(x) = (x-c)^2$ which means that $a = -2c$ and $b = c^2$.

4. Polynomial Interpolation

Let $p(x)$ be a polynomial of degree at most 2 such that $p(-1) = 3, p(0) = 1, p(1) = 2$.

(a) Find the coefficients of $p(x)$ by solving a system of linear equations.

(b) Find the coefficients of $p(x)$ using the Lagrange interpolation.

$p(x) = \frac{3}{2}x^2 - \frac{1}{2}x + 1$.

5. Surjection, Injection, Bijection

Are the following functions ("mod" here is an operation) surjective, injective, and/or bijective?

(a) $f(x) = x^3 \bmod 3$, with domain $A = \{0,1,2\}$ and range $B = \{0,1,2\}$.

Surjective, injective, and bijective.

(b) $f(x) = x^3 \bmod 3$, with domain $A = \{0,1,2,3\}$ and range $B = \{0,1,2\}$.

Surjective.

(c) $f(x) = x^3 \bmod 3$, with domain $A = \{0,1,2\}$ and range $B = \{0,1,2,3\}$.

Injective.

(d) $f(x) = x^3 \bmod 4$, with domain $A = \{0,1,2,3\}$ and range $B = \{0,1,2,3\}$.

None.