MATH 918, Number Theory and Cryptography July 17, 2003

Assignment I

Time: 1:15-3:15, MTWR
Instructor : Jon-Lark Kim

This assignment is due on July 23 (Wednesday). You can discuss the problems but write down your own answer. Show your work logically and write neatly. The following sections refer to Koblitz's A Course in Number...

Problem 1. Convert $\sqrt{5} = 2.236067...$ to the base-2 number.

Problem 2. Show that if $\lim_{n\to\infty} f(n)/g(n)$ is finite, then $f = O(g)$, where f and g are positive functions on natural numbers.

Problem 3. Using the big-0 notation, estimate the number of bit operations required to multiply an $r \times n$-matrix by an $n \times s$-matrix, where all matrix entries are bounded by m. (Ex. 12 in Sec. I.1)

Problem 4. Let n be a very large integer written in binary. Find a simple algorithm that computes $[\sqrt{n}]$ in $O(\log^3 n)$ bit operations. (Ex. 16 in Sec. I.1)

Problem 5. The purpose of this problem is to find a general estimate for the time required to compute $gcd(a, b)$ $(a > b)$ that is better than $O(\log^3 a)$.
(a) Show that the number of bit operations required to perform a division $a = qb + r$ is $O((\log b)(1 + \log q))$.
(b) Applying (a) to all of the $O(\log a)$ divisions of the form $r_{i-1} = q_{i+1}r_i + r_{i+1}$, derive the total time estimate $O((\log b)(\log a))$. (Ex. 11 in Sec. I.2.)

Problem 6. Find the smallest nonnegative solution of the following system of congruences. $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod{11}$, $x \equiv 5 \pmod{16}$. (Ex. 11 (a) in Sec. I.3.)

Problem 7. Let $m = 7785562197230017200 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 181$. Find the least nonnegative residue of $6647^{362} \pmod m$. (Ex. 21 (a) in Sec. I.3.)

Problem 8. (a) Prove $\prod_p \frac{1}{1-\frac{1}{p}}$ diverges to infinity, where the product takes all primes p.
(b) Using (a), prove that the sum of the reciprocals of the primes diverges.
(c) Find a sequence n_j approaching ∞ for which $\lim_{j\to\infty} \frac{\varphi(n_j)}{n_j} = 1$ and a sequence n_j for which $\lim_{j\to\infty} \frac{\varphi(n_j)}{n_j} = 0$. (Ex. 23 in Sec. I.3.)

Problem 9. Prove that if $2^n - 1$ is a prime, called *a Mersenne prime*, then n must be a prime too. Prove that if $2^n + 1$ is a prime, called *a Fermat prime*, then n must be a power of 2. (Ex. 2 in Sec. I.4.)

Good Luck !

MATH 918, Number Theory and Cryptography July 24, 2003

Assignment II

Time: 1:15-3:15, MTWR
Instructor : Jon-Lark Kim

This assignment is due on Aug 1 (Friday). Put your homework in my mailbox. You can discuss the problems but write down your own answer. Show your work logically and write neatly. The following sections refer to Koblitz's A Course in Number...

Problem 1. Suppose that f is a power of a prime l. Find a simple formula for the number of monic irreducible polynomials of degree f over $\mathbb{F}_p$. (Ex. 6, Sec II.1)

Problem 2. Suppose that $\alpha \in \mathbb{F}_{p^2}$ satisfies $X^2 + aX + b$, where a, b are in $\mathbb{F}_p$.
(a) Prove that α^p also satisfies this polynomial.
(b) Prove that if $\alpha \notin \mathbb{F}_p$, then $a = -\alpha - \alpha^p$ and $b = \alpha^{p+1}$.
(c) Prove that if $\alpha \notin \mathbb{F}_p$ and $c, d \in \mathbb{F}_p$, then $(c\alpha + d)^{p+1} = d^2 - acd + bc^2 \in \mathbb{F}_p$.
(d) Let i be a square root of -1 in $\mathbb{F}_{19^2}$. Use part (c) to find $(2 + 3i)^{101}$ in the form $a + bi,\ a, b \in F_{19}$. (Ex. 9, Sec II.1)

Problem 3. We want to evaluate the Legendre symbol $\left(\frac{1801}{8191}\right)$ in the following two ways.
(a) Use the reciprocity law only for the Legendre symbol (i.e. factoring all numbers that arise), and
(b) Use the reciprocity law for the Jacobi symbol without factoring any odd integers. (Ex. 10, Sec II.2)

Problem 4. Let $p = 2081$, and let n be the smallest positive nonresidue $\pmod p$. Find n, and use the method in the text to find a square root of $302 \pmod p$. (Ex. 19, Sec II.2)

Problem 5. You intercept the ciphertext "OFJDFOHFXOL", which was enciphered using an affine transformation of single-letter plaintext units in the 27-letter alphabet (with blank= 26). You know that the first word is "I " ("I" followed by blank). Determine the enciphering key, and read the message.

Good Luck !

MATH 918, Number Theory and Cryptography Aug. 5, 2003

Assignment III

Time: 1:15-3:15, MTWR
Instructor : Jon-Lark Kim

This assignment is due on Aug 13 (Wednesday). You can discuss the problems but write down your own answer. Show your work logically and write neatly. The following sections refer to Koblitz's A Course in Number...

Problem 1. Using Ex 16-18, Sec III.2, find a formula for the number of elements in the set $M_2(\mathbb{Z}/N\mathbb{Z})^*$ of invertible matrices mod N. Write your formula for the number of invertible 2 by 2 matrices in $M_2(\mathbb{Z}/N\mathbb{Z})^*$ in a similar form for the number $\varphi(N) = N\prod_{p|N}(1-\frac{1}{p})$. How many possible 2×2 enciphering matrices A are there when $N = 26, 29, 30$? (Ex 19, Sec III.2)

Problem 2. Suppose that the following 40-letter alphabet is used for all plaintexts and ciphertexts: A–Z with numerical equivalents 0–25, blank=26, .=27, ?=28, $=29, the numerals 0-9 with numerical equivalents 30–39. Suppose that plaintext message units are digraphs and ciphertext messages units are trigraphs (i.e., $k=2,\ l=3,\ 40^2 < n_A < 40^3$ for all n_A).
(a) Send the message "SEND $7500" to a user whose enciphering key is $(n_A, e_A) = (2047, 179)$.
(b) Break the code by factoring n_A and then computing the deciphering key (n_A, d_A). (Ex 1, Sec IV.1)

Problem 3. Using the Silver-Pohlig-Hellman algorithm, find the discrete log of 153 to the base 2 in $\mathbb{F}_{181}^*$. (note : 2 is a generator of $\mathbb{F}_{181}^*$.) (Ex 10, Sec IV.3)

Problem 4. (bonus) If there are 23 people in a classroom, then the probability that two of them have the same birthday is slightly more than 50%! If there are 30, the probability is around 70%. This phenomenon is called the *birthday paradox*. For 23 people, we can compute the probability as follows; $1 - \left(1-\frac{1}{365}\right)\left(1-\frac{2}{365}\right)\cdots\left(1-\frac{22}{365}\right) = .507$.
(a) Justify this argument. Using 17 people in our Crypto class, compute the probability that two of them have the same birthday.
(b) Discrete log problem can be solved with high probability by a birthday attack as follows. Let p be a large prime and want to find x such that $b^x \equiv y \pmod{p}$. Make two lists, both of length around $\sqrt{p}$.

1) The first list contains numbers $b^k \pmod{p}$ for about $\sqrt{p}$ random values of k.
2) The second list contains numbers $yb^{-l} \pmod{p}$ for about $\sqrt{p}$ random values of l.

Show that how one can use the birthday attack to solve the discrete log problem, i.e. how to get $x \equiv ind(y) \pmod{p-1}$ with a high probability.

Have a good summer!