Math 1580 – Problem Set 4. Due Friday Oct. 7, 4pm

Typo fixed 10/5 in problem 4.

Problem 1. Let p and q be distict primes and let e and d be integers satisfying

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

Suppose further that c is an integer with $\gcd(c, pq) > 1$. Prove that

$$x \equiv c^d \pmod{pq} \quad \text{is a solution to} \quad x^e \equiv c \pmod{pq}$$

thereby completing the proof of Proposition 3.4.

Problem 2. Recall that

$$\phi(N) = \#\{1 \le k < N : \gcd(k, N) = 1\}.$$

(a) Prove a formula for $\phi(p^j)$ when p is prime. (Hint: which values of k between 1 and $p^j - 1$ are *not* coprime to p^j? It may help to do some examples first.)

(b) Prove that if M and N are coprime, then

$$\phi(MN) = \phi(M)\phi(N).$$

(In particular, $\phi(pq) = (p-1)(q-1)$ when p and q are distinct primes.)

(c) Use the results of the previous two parts to show that for general N,

$$\phi(N) = N \prod_{p|N} \left(1 - \frac{1}{p}\right)$$

where the product is over the distinct primes p which divide N.

(d) Prove *Euler's formula*

$$a^{\phi(N)} \equiv 1 \pmod{N} \quad \text{for all } a \text{ such that } \gcd(a, N) = 1.$$

(Hint: Mimic the proof of Fermat's little theorem, but instead of looking at all multiples of a, just take the multiples ka for all values of k satisfying $\gcd(k, N) = 1$.)

Problem 3. Let N, c, and e be positive integers satisfying $\gcd(N, c) = 1$ and $\gcd(e, \phi(N)) = 1$.

(a) Explain how to solve the congruence

$$x^e \equiv c \pmod{N}$$

assuming that you know the value of $\phi(N)$.

(b) Solve the following congruences.

(i) $x^{577} \equiv 60 \pmod{1463}$. Note $1463 = 7 \cdot 11 \cdot 19$.

(ii) $x^{133957} \equiv 224689 \pmod{2134440}$. Note $2134440 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11^2$.

(iii) $x^{103} \equiv 317730 \pmod{2038667}$. Note $2038667 = 1301 \cdot 1567$.

Problem 4. A *decryption exponent* for an RSA public key (N, e) is an integer d with the property that $a^{de} \equiv a \pmod{N}$ for all integers a coprime to N.

(a) Suppose that Eve is able to obtain decryption exponents for a fixed modulus N and for a large number of different encryption exponents e. Explain how Eve can use this information to try and factor N.

(b) Let $N = 38749709$. Eve obtains the following encryption/decryption exponent pairs:

$$(e_1, d_1) = (10988423, 16784693), \quad (e_2, d_2) = (25910155, 11514115)$$

Use this information to factor N.

(c) Let $N = 225022969$. Eve obtains the following encryption/decryption exponent pairs:

$$(70583995, 4911157), \quad (173111957, 7346999), \quad (180311381, 29597249)$$

Use this information to factor N.

Problem 5. We stated that 561 is a Carmichael number, but we never checked that $a^{561} \equiv a \pmod{561}$ for every value of a.

(a) The number 561 factors as $3 \cdot 11 \cdot 17$. First use Fermat's little theorem to prove that

$$a^{561} \equiv a \pmod{3}, \quad a^{561} \equiv a \pmod{11}, \quad a^{561} \equiv a \pmod{17}$$

for every value of a. Then explain why these congruences imply that $a^{561} \equiv a \pmod{561}$ for every a.

(b) Show similarly that $1024651 = 19 \cdot 199 \cdot 271$ is a Carmichael number.

(c) Prove that a Carmichael number must be odd.

(d) Prove that a Carmichael number must be a product of *distinct* primes. (Hint: use your result from Problem 2.(a).)

Problem 6. Use the Miller-Rabin test on each of the following numbers. In each case, either provide a Miller-Rabin witness for the compositeness of n, or conclude that n is probably prime by providing 10 numbers that are not Miller-Rabin witnesses for n.

(a) $n = 294409$

(b) $n = 118901509$

(c) $n = 118901521$

(d) $n = 118901527$

Problem 7. Extra credit: Suppose that for a given N, Eve obtains a single encryption/decryption exponent pair. Show how the basic idea in the Miller-Rabin primality test can be applied to use this information to factor N.

Hint for the whole problem set: If in doubt, think about the Chinese Remainder Theorem.