

Mathematics 170: Ideas in Mathematics

Homework 3

This assignment is due Thursday, June 4, 2009, at the beginning of class. Please hand the homework in in class. If you can't make it to class, place it in my mailbox in the departmental office (DRL 4W1) or bring it to my office (DRL 4N27). You are allowed to talk about the homework with each other, but please write it up alone.

For reference, I'll remind you how the RSA algorithm works. Let's say you would like to be able to encode messages; then you do the following.

1. Choose two distinct primes p and q . (These are usually of similar size, and large; in our examples they will be small.)
2. Compute $n = pq$; this will be the modulus.
3. Compute $\phi(n) = (p-1)(q-1)$, the *totient* of n . This is the number of numbers among $1, 2, \dots, n-1$ which have no factor in common with n .
4. Choose an exponent e such that $1 < e < \phi(n)$, where e and $\phi(n)$ are relatively prime. e is the *encoding exponent*.
5. Find d such that $de \equiv 1 \pmod{\phi(n)}$, by either trial and error or the Euclidean algorithm. d is called the *decoding exponent*.

Then the *public key* (which is used to encode messages to be sent to you) is the pair of numbers (n, e) ; the *private key* is the single number d . To encrypt the message W , compute $C = W^e \pmod{n}$, and send that. To decode the ciphertext C , compute $C^d \pmod{n}$. This will be W .

1. Let $n = 65$ be the modulus in the RSA algorithm.
 - (a) If $n = pq$, where p and q are prime, what are p and q ? What is $\phi(n)$?
 - (b) Let $e = 11$ be the encoding exponent. What is the corresponding decoding exponent d ?
2. Let W be the plaintext message 3. Using the public key $(n, e) = (65, 11)$ from Problem 1, encode this message.
3. Let C be the ciphertext message 7. Using the private key you found in Problem 1(b), decode this message.
4. Compute $5^{173} \pmod{7}$ and $8^{1522} \pmod{11}$, using Fermat's little theorem.
5. Compute $5^{173} \pmod{8}$ and $8^{1522} \pmod{15}$, using Euler's theorem.
6. Show that $\sqrt{2} + \sqrt{7}$ is irrational. (B+S 2.6.14) Bonus: show that $\sqrt{p} + \sqrt{q}$ is irrational for any primes p and q . (B+S 2.6.38). You may use the result of 2.6.37, that \sqrt{pq} is irrational for any two different prime numbers p and q , if you wish.
7. Show that the sum of any two rational numbers is another rational number. (B+S 2.6.22)
8. Let a and b be any two irrational numbers. Show that either $a+b$ or $a-b$ is irrational. Hint: what happens if both $a+b$ and $a-b$ are rational? (B+S 2.6.40)