

**MATH 4450/6450**  
**HOMEWORK 4**  
**DUE 2/9/07**

Do the following book problems:

**3.13:** 25, 29, 32.

**6.8:** 12, 19, 28.

**6.9:** 4, 5, 10.

Your instructions for the extra problems this week are: 4450 students need only do extra problems 1 and 2. As usual, 6450 students have to do everything.

**Extra problem 1:** In  $\mathbb{Z}_n^*$ , we define a primitive root to be an element  $g \in \mathbb{Z}_n^*$  such that the powers of  $g$  give all the elements of  $\mathbb{Z}_n^*$ . Alternatively, we could have defined it to be an element  $g \in \mathbb{Z}_n^*$  whose multiplicative order is  $\phi(n)$ . (We have seen this concept when  $n$  is prime, but it extends naturally to the composite case.) For the rest of this problem, assume that  $p$  is an odd prime. We're going to show that there is a primitive root mod  $p^2$ .

(a) To warm up, show that there are no primitive roots mod 8.

(b) Suppose that  $g$  is a primitive root mod  $p$  for some positive integer  $k$ . Show that the order of  $g$  in  $\mathbb{Z}_{p^2}$  is either  $p-1$  or  $p(p-1)$ . (In the latter case,  $g$  is a primitive root mod  $p^2$ .)

(c) Assuming that  $g^{p-1} \equiv 1 \pmod{p^2}$ , expand out  $(g+p)^{p-1} \pmod{p^2}$  by the binomial theorem, and use this to show that  $(g+p)^{p-1}$  is not congruent to 1 mod  $p^2$ .

(d) So use part (c) to show that if  $g$  is not a primitive root mod  $p^2$ , then  $g+p$  is a primitive root mod  $p^2$ .

*Remarks:* It turns out that there is a primitive root mod  $n$  if and only if  $n = 4$  or  $p^k$  or  $2p^k$  for some odd prime  $p$ . The hard part (or at least one of the hard parts) is adapting the above argument to show that if  $g$  is a primitive root mod  $p^k$ , then either  $g$  or  $g+p$  is a primitive root mod  $p^{k+1}$ .

**Extra problem 2:** Recall that  $n$  is said to be a *Carmichael number* if  $a^{n-1} \equiv 1 \pmod{n}$  for all  $a \in \mathbb{Z}_n^*$ . (The book's definition in Exercise 3.13.16 is equivalent; you might want to think about why.) So suppose that  $n$  is a Carmichael number. Using the result of extra problem 1, show that  $n$  cannot be divisible by  $p^2$ , where  $p$  is prime. (Hint: Let  $g$  be a primitive root mod  $p^2$ . Then the order of  $g$  mod  $n$  is divisible by  $p$  (why?); combine this with  $g^{n-1} \equiv 1 \pmod{n}$  to get a contradiction.)

**Extra problem 3:** Suppose that the Miller-Rabin test shows that  $n$  is composite, for a certain choice of  $a$ . Then we call  $a$  a *Miller-Rabin witness* to the compositeness of  $n$ . (In other words, if  $n$  is composite and  $a$  is *not* a Miller-Rabin witness, then  $n$  is a strong  $a$ -pseudoprime, as in Exercise 6.9.13.) Here we will show that every composite  $n$  has at least one Miller-Rabin witness.

(a) To warm up, explain why  $a$  is a Miller-Rabin witness for  $n$  if  $a^{n-1} \not\equiv 1 \pmod n$ . So from now on, we'll suppose that  $n$  is a Carmichael number (otherwise we're already done).

(b) In the Miller-Rabin test, we write  $n-1 = 2^k m$  where  $m$  is odd, and create the numbers  $b_i$ . Show that if  $n$  is a Carmichael number and  $a$  is not a Miller-Rabin witness for  $n$ , then there is some  $j(a) \leq k-1$  such that  $b_{j(a)} \equiv -1 \pmod n$ , unless  $b_0 \equiv 1$  (in which case we say that  $j(a) = -\infty$ ). (Hint: Nothing to it; just read the test!)

(c) Suppose, then, that  $n$  is a Carmichael number, so that by Extra Problem 2  $n = yz$  with  $y, z > 1$  and  $\gcd(y, z) = 1$ , and suppose that  $n$  has no Miller-Rabin witnesses. Let  $v \in \mathbb{Z}_n^*$  be chosen so that  $j(v)$  is at least as big as  $j(w)$  for any  $w \in \mathbb{Z}_n^*$ . Use the Chinese Remainder Theorem to construct an element  $x \in \mathbb{Z}_n^*$  such that  $x \equiv v \pmod y$  and  $x \equiv 1 \pmod z$ . Why is this a contradiction? (Hint:  $x^{2^{j(v)}m}$  is  $\equiv -1 \pmod y$  and  $1 \pmod z$ , so it can't be  $-1$  or  $1 \pmod n$ ...)

*Remarks:* If you know a little group theory, you can adapt this argument to show that for any composite  $n$ , at least half of the elements of  $\mathbb{Z}_n^*$  are Miller-Rabin witnesses for  $n$ . In fact, it is known that at least  $3/4$  of the elements of  $\mathbb{Z}_n^*$  are Miller-Rabin witnesses for  $n$  (and apparently this bound is sharp for the Carmichael number  $n = 8911$ ). This is not such great news for deterministic primality testers, though, since you still won't know for sure if  $n$  is prime until you've tested about  $n/4$  numbers. If you are willing to assume something called the "Generalized Riemann Hypothesis," then you are guaranteed that there will be a Miller-Rabin witness in the first  $2(\ln n)^2$  numbers mod  $n$ , or your money back (i.e.  $n$  is prime).

**Extra Problem 4:** Similarly to Extra Problem 3, we say that  $a$  is a Solovay-Strassen witness to the compositeness of  $n$  if  $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod n$ . Here we will show that every composite  $n$  has at least one Solovay-Strassen witness.

(a) Again, warm up by explaining why  $a$  is a Solovay-Strassen witness for  $n$  if  $a^{n-1} \not\equiv 1 \pmod n$ . (Hint: Two numbers can't be congruent mod  $n$  if their squares aren't!)

(b) So suppose that we can write  $n = pz$  with  $p$  an odd prime,  $p \nmid z$ . Let  $b$  be a quadratic nonresidue mod  $p$ . Use the Chinese Remainder Theorem to construct a number  $a$  such that  $a \equiv b \pmod p$  and  $a \equiv 1 \pmod z$ . Show that  $a$  is a Solovay-Strassen witness for  $n$ . Since every Carmichael number can be written in the above form, we are done.

*Remark:* Again, one can adapt this argument to show that at least half of the numbers in  $\mathbb{Z}_n^*$  are Solovay-Strassen witnesses for  $n$ , and again the test becomes just as fast as the Miller-Rabin test if you assume the Generalized Riemann Hypothesis.