

## MATH 470 Homework 6

[1] Consider the “candidate prime”  $n = 15841$ .

- a. Use Fermat’s test (“for a random integer  $a$  with  $1 < a < n - 1$ ; if  $a^{n-1} \not\equiv 1 \pmod{n}$ , then  $n$  is composite, else  $n$  is probably prime”) to check the value of  $n$ , taking in turn  $a = 2, 3, 5, 7$ .
- b. Use the Solovay-Strassen test on  $n$  with bases  $a = 2, 3, 5$  (“For a random integer  $a$  with  $1 < a < n - 1$ ; if  $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$  then  $n$  is composite, else  $n$  is probably prime”).
- c. Now use the Miller-Rabin test on this  $n$ , taking bases  $a = 2$  then  $a = 3$ .

[Code for taking modular exponentials, calculating the Jacobi symbol, and the Miller-Rabin test is available from the class web page.]

This is one tough composite! You should have found that both the Fermat and Solovay-Strassen tests find this to be a “prime” i.e a *pseudoprime* for the witnesses  $a = 2, 3, 5$  (who are therefore “liars” for  $n$ ).  $n = 15841$  is also a *strong pseudoprime* for  $a = 2$  with the Miller-Rabin test. But this test shows  $n$  to be composite for any of  $a = 3, 5, 7$ . We aren’t restricted to just prime values of the witness  $a$ , but if try the Miller-Rabin test with  $a = 4, 8$  we see it also identifies  $n = 15841$  as prime. Note: you aren’t going to be required here to show all the steps of the gory calculations of the modular exponentations - but the value of the main “idea steps” should be shown.

There is a lesson here: choosing different witnesses doesn’t guarantee independence of results - in fact if one of these test fails for  $a$  (gives a pseudoprime) then it is more likely to also fail for witnesses containing  $a$  as a factor. For this reason, the widely-used Miller-Rabin test is often implemented using the first  $t$  primes as witnesses. Note also, the apparent superiority of the Miller-Rabin test over the Solovay-Strassen test. This can be deceiving. Miller-Rabin is considerably faster to implement (meaning we can check more witnesses in a given time frame and hence greater likelihood of success) and won’t give “fail” when Solovay-Strassen gets it correct (that is  $a$  cannot be a true witness for Solovay-Strassen but a liar for Miller-Rabin). However, if  $n \equiv 3 \pmod{4}$  then the two tests have identical liars. Note that  $15841 \equiv 1 \pmod{4}$ .

[2] Let  $p$  and  $q$  be distinct odd primes, and let  $n = pq$ . Suppose  $y$  is such that  $\gcd(y, n) = 1$ .

- a. Show that  $y^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{p}$  and  $y^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{q}$
- b. Deduce that  $y^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{n}$
- c. Suppose now  $e$  and  $d$  are such that  $ed \equiv 1 \pmod{\frac{1}{2}\phi(n)}$  then  $y^{ed} \equiv y \pmod{n}$ .

[This problem shows that we could also compute  $d$  by the relation  $ed \equiv 1 \pmod{\frac{1}{2}\phi(n)}$  in RSA].

For the first part note that  $\phi(n) = (p - 1)(q - 1)$  and since  $q - 1$  is even,  $q - 1 = 2k$  for some integer  $k$ . Now  $y^{\frac{1}{2}\phi(n)} = y^{(p-1)k} = (y^k)^{p-1} \equiv 1 \pmod{p}$  by Fermat’s theorem. Same for  $q$ . From part a) we have the two congruences  $y^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{p}$ ,  $y^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{q}$  and so we can combine these by the Chinese Remainder Theorem into a congruence  $\pmod{pq}$  in a unique way - and this is clearly  $y^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{n}$ . Part c) is now immediate:  $ed = 1 + \frac{1}{2}\phi(n) \cdot r$  for some integer  $r$  and so  $y^{ed} \equiv y^{1 + \frac{1}{2}\phi(n) \cdot r} \equiv y \cdot (y^{\frac{1}{2}\phi(n)})^r \equiv y \cdot 1^r \equiv y \pmod{n}$

- [3] Try to factor  $n = 1545013$  by using Fermat factorisation: (“compute  $n + 1^2, n + 2^2, n + 3^2, \dots$ , until we find a square.”).

First note that  $\sqrt{n} = 1242.99$  and so  $\lfloor n \rfloor = 1442$ . Note that  $1243^2 = 1545049$  and  $1244^2 = 1547536$ . Now  $1545013 + 1^2 = 1545014 < 1243^2$  so  $n + 1^2$  isn't a square. Similarly,  $1545013 + 2^2 = 1545017$ ,  $1545013 + 3^2 = 1545022$ ,  $1545013 + 4^2 = 1545029$ ,  $1545013 + 5^2 = 1545038$  and these also fail to give a complete square. However, at the next try,  $1545013 + 6^2 = 1545049 = 1243^2$ , Thus  $1545013 = (1243 + 6)(1243 - 6) = 1237.1249$  and we have factored  $n$ .

- [4] Use the  $p - 1$  factoring method to compute the factors of:

a  $n = 17513$ . Depending on how you code this you may have to compute  $b = a^{B!} \pmod{n}$  by using the sequence  $b_1 = a \pmod{n}$ ,  $b_j = b_{j-1}^j \pmod{n}$  for  $j = 2, \dots, B$ . Simply compute  $d = \gcd(b, n)$  to see if you get a nontrivial factor. Only a modest, single digit value of  $B$  is needed here so you should show all the steps of the calculation.

b  $n = 8834884587090814646372459890377418962766907$ .

[This will test your code, but see the Maple worksheet from the web page which will work this problem instantly. Just provide the factors of  $n$ ].

For part a) try  $B = 6$  so that  $6! = 720$  and  $2^{720} \pmod{n}$  is easily computed to give  $b = 13648$ . ( $2^{720} = 2^{512+128+64+16}$  and we can very quickly compute each of these powers by successive squaring.) Now compute  $\gcd(b - 1, n)$ . This equals 1, so  $B = 6$  fails.  $2^{7!} \pmod{n}$  is just  $(2^{6!})^7 \pmod{n} = 13648^7 \pmod{n}$  and by successive multiplications we get, corresponding to  $B = 7$ ,  $b = 11817$ . Computing  $\gcd(b - 1, n)$  gives 211 and so we have found a factor of  $n$ .

- [5]  $n = 642401$ . Suppose you discover from runs of the sieve that  $516107^2 \equiv 7 \pmod{n}$  and  $187722^2 \equiv 2^2 \cdot 7 \pmod{n}$ . Use this information to factor  $n$ , explaining your steps.

Note that if  $a = 516107$ ,  $b = 187722$  then  $(2a)^2 \equiv b^2 \equiv 7 \pmod{n}$  and so  $(2a - b)(2a + b) \equiv 0 \pmod{n}$ . Also,  $2a \not\equiv b \pmod{n}$  and  $2a \not\equiv -b \pmod{n}$ . Thus  $\gcd(2a - b, n)$  must yield a nontrivial factor of  $n$ . We compute this to get  $\gcd(2a - b, n) = 1129$ . Note that  $\gcd(2a + b, n) = 569$  and that  $n = 569 \cdot 1129$ .

- [6] Alice has an idea to increase the security of her RSA code. So she doesn't have to generate such large primes, she is going to use an  $n$  that has three prime factors  $n = pqr$ . There is a single  $e$  and  $d$  as before with  $ed \equiv 1 \pmod{\phi(n)}$ . Suppose Bob sends her a message using her system with the convention that the alphabetic message is converted to an integer via space=00,  $a = 01$ ,  $b = 02, \dots, z = 26$ . (Thus “bob” becomes 011501 and “you and I” is 251521000114040009). The encrypted message is 13480622. Alice's public parameters are  $e = 7$  and  $n = 43379579$  (with private prime factors of 89, 601, 811). Can you decrypt Bob's message to Alice?

Here we have to solve the congruence  $ed \equiv 1 \pmod{\phi(n)}$  to compute  $d$  from  $e$ . In this case it is  $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$  or  $ed \equiv 1 \pmod{88.600.810}$ . Thus  $d = 1/7 \pmod{42768000}$  and we can use the Euclidean algorithm to see that  $d = 18329114$ . Now  $c^d \equiv 13480622^{18329114} \pmod{43379579}$  and while formidable by hand is easily computed via the C code or Maple code to produce  $m = 15110125 = \text{“okay”}$ .

[7] Show that  $a = 2$  is a primitive root of  $p = 13$ . Calculate the discrete logarithms  $(\text{mod } 13)$  base 2 of  $\beta = 5$  and  $\beta = 7$ , that is  $L_2(5)$ ,  $L_2(7)$ .

First part is simply a check that  $2^k \pmod{13}$  gives distinct values for  $k = 1, 2, \dots, p-1$ . There is a much better way for larger values of  $p$ , but that is another story. For the second part, given the really small numbers involved, the simplest way is just to look at the powers generated in the first part to get the answer. But that is not the purpose.

Let  $N := \sqrt{13} \approx 4$ . Take  $\beta := 5$ . We compute  $2^j \pmod{13}$  and  $\beta \cdot 2^{-Nk} \pmod{13}$  for  $j, k = 0, 1, \dots, N-1$ . The first sequence (“baby steps”) is just 1, 2, 4, 8. Since  $2 \cdot 7 \equiv 1 \pmod{13}$  we have  $2^{-N} \equiv 7^N \equiv 7^4 \equiv 49 \cdot 49 \equiv (-3)(-3) \equiv 9 \pmod{13}$ . The “giant steps” are therefore  $5 \cdot 9^k \pmod{13}$  for  $k = 0, 1, 2, 3$  or 5, 6, 2, 5. These two lists indeed have an element in common - the number 2 corresponding to  $j = 1$  and  $k = 2$ . Thus  $5 \cdot 2^{-2N} \equiv 2^1 \pmod{13}$  or  $5 \equiv 2^{2N+1} \equiv 2^9 \pmod{13}$ . Thus  $x = 9$ .

$p-1 = 12 = 2^2 \cdot 3$  so use Pohlig-Hellman. Take  $\beta = 7$ . Then  $z_2 = 2^{(p-1)/2} \equiv 2^6 \equiv 64 \equiv -1 \pmod{13}$  and  $z_3 = 2^{(p-1)/3} \equiv 2^4 \equiv 3 \pmod{13}$ . Also  $\beta^{(p-1)/2} = 7^6 \equiv (-3)^3 \equiv -27 \equiv -1 \pmod{13}$  while  $\beta^{(p-1)/3} = 7^4 \equiv (-3)^2 \equiv 9 \pmod{13}$ .

$x_2 = c_0 + 2c_1$  with  $c_i \in \{0, 1\}$ . Then  $-1 \equiv \beta^{(p-1)/2} \equiv z_2^{c_0} \equiv (-1)^{c_0}$  so that  $c_0 = 1$ . Let  $\beta_1 \equiv \beta \cdot 2^{-1} \equiv 7 \cdot 7 \equiv 10 \pmod{13}$ . Then  $\beta_1^{(p-1)/4} \equiv 10^3 \equiv (-3)^3 \equiv -27 \equiv -1 \pmod{13}$ , so that  $z_2^{c_1} \equiv (-1)^{c_1} \equiv -1 \pmod{13}$  and hence  $c_1 = 1$ . Thus  $x_2 \equiv c_0 + 2c_1 \equiv 3 \pmod{4}$ .  $x_3 = c_0$  with  $c_0 \in \{0, 1, 2\}$  and so  $z_3^{c_0} \equiv 3^{c_0} \equiv \beta^{(p-1)/3} \equiv 9 \pmod{13}$  so that  $c_0 = 2$ . Then  $x_3 = 2$ .

Then the solution  $x$  satisfies both  $x \equiv 3 \pmod{4}$  and  $x \equiv 2 \pmod{3}$ . The Chinese Remainder Theorem then gives that  $x \equiv 11 \pmod{12}$  and so we have  $2^{11} \equiv 7 \pmod{13}$ .