

1. TAKE-HOME TEST 6

Due : last day of classes

Collaborative

This time you have a choice. Do any **five** of the following six problems.

- (1) (a) How many positive integers are less than 3200 and relatively prime to 3200?
- (b) How many positive integers are less than 9600 and relatively prime to 3200? (Provide a sentence or two of justification here.)
- (c) Find the last four digits of $3^{2,394,592,093,230}$. For this part, be sure to show your work and to cite clearly any results you use. You may use your calculator to square, multiply, and divide but that's it. Show your work carefully, noting when and how you used your calculator.
- (2) If n is the product of two distinct primes p and q , and we know the values of p and q , then we proved in class that $\phi(n) = (p-1)(q-1)$. Find formulas for p and q in terms of n and $\phi(n)$. Thus, if you know n and $\phi(n)$ (and you know n has the form pq) then you can factor n . Show that your method for finding p and q works by using the fact that $\phi(31325369) = 31313280$ to factor 31325369. Hint: Start by showing that, in general, if $n = pq$ with $p > q$ then $p + q = n - \phi(n) + 1$ and $p - q = \sqrt{(p+q)^2 - 4n}$.
- (3) An investigative reporter came across the following message recently. He says that he was told it was encoded using something called RSA public key cryptography with keys $e = 3299$ and $n = 4171$. He has no idea what this means. Can you decode it for him? Be sure to explain exactly what you did to decode the message. (To save you some time, it may be helpful to have a calculator or a computer which can handle a large number of digits, although you can do this problem with nothing more than a TI-86. Incidentally, the 'mod' function on the TI-86 is highly erratic and may not give you the correct answer, so be careful!)

1214 0556 3545 4089 1604 1128 1631 0313 3205 1004 1490 3646

- (4) Most of you conjectured on the last exam that if p is an odd prime and $o_p(a) = p-1$, then $o_p(p-a)$ is either $p-1$ or $(p-1)/2$, depending on whether p is congruent to 1 or 3 modulo 4, respectively. Prove this statement. Hint: First prove that if $o_p(a) = p-1$ then $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. (Problem 5(a) on Test #5 is helpful here.) Also, note that as $p-a \equiv -a \pmod{p}$, then $(p-a)^k \equiv (-1)^k a^k \pmod{p}$. Finally, show that $(-1)^{\frac{p-1}{2}}$ is -1 if $p \equiv 3 \pmod{4}$ and 1 if $p \equiv 1 \pmod{4}$.
- (5) (a) Make a list of values of $\phi(n)$ for $3 \leq n \leq 50$.
- (b) All the values of $\phi(n)$ in your list should be even. Explain why this is always true. In other words, explain why $\phi(n)$ is even for every $n > 2$.
- (c) In fact, it should appear from your list that $\phi(n)$ is "usually" divisible by 4. State a conjecture of the form " $\phi(n)$ is divisible by 4 if and only if *(fill this in)*", where the blank is filled in with some conditions on the prime factorization of n . You can earn bonus points by proving part or all of your conjecture.
- (6) There has been a great curiosity about numbers all of whose digits are equal to 1, that is, numbers of the form 1, 11, 111, 1111, etc. They are

called repunits (*repeating units*). We shall denote the repunit consisting of a sequence of n ones by R_n . A helpful observation is that

$$R_n = 11 \dots 111 = \frac{10^n - 1}{9}$$

- (a) Show that no repunit is divisible by 2 or 5. (This one's a gimme!)
- (b) Show that there are infinitely many repunits which are divisible by 3.
- (c) Prove that for each prime p except 2 and 5, there is some repunit R_n which is divisible by p . (Hint: Fermat's Theorem is very useful here.)
- (d) Is it true that for each prime p except 2 or 5 there are infinitely many repunits divisible by p ? Give a proof or a counterexample.
- (e) (*Bonus Points*) Prove that for any positive integer m which is relatively prime to 30 there is a repunit which is divisible by m . (Hint: Euler's Theorem!)