

Prime Numbers and Cryptography

Mathematical Explorations – Math 110

Block 2, Fall 2007

Here is a list of all the primes less than 100 (there are 25 of them):

2 3 5 7 11 13 17 19 23 29 31 37 41
43 47 53 59 61 67 71 73 79 83 89 97

1. How many primes are of the form $4k + 1$? How many primes are of the form $4k + 3$? Can you guess about what percent of primes will be in each category? Do the same for $6k + 1$ and $6k + 5$.
2. For each prime p less than 100, try to write p as $x^2 + y^2$ for some integers x and y . Can you make a guess for which primes this will be possible? Try this for $x^2 + 2y^2$ and $x^2 + 3y^2$.
3. For each of the values of n below, calculate the proportion of primes less than n and $\frac{1}{\ln n}$. Is $\frac{1}{\ln n}$ a good approximation for the percentage of primes less than n ?

n	# of primes less than n	% of prime #'s less than n	$\frac{1}{\ln n}$
10	4		
100	25		
1000	168		
10,000	1229		
100,000	9592		
1,000,000	78,498		
10,000,000	664,579		
100,000,000	5,761,455		
1,000,000,000	50,847,534		

4. Your friend wants to send you a secret number D between 0 and 10000. You tell him to compute $E \equiv D^{589} \pmod{10001}$, and he tells you the answer $E = 864$. You know that if you compute $E^{133} \pmod{10001}$, you'll get the secret number D . What is it?
(Hint: Compute $E^2 \pmod{10001}$, $E^4 \pmod{10001}$, ... using a calculator).
5. Another popular cryptosystem is called the Diffie-Hellman Key Exchange. Alice and Bob decide on a prime number $p = 101$ and a certain base number $g = 2$. Alice chooses a random secret number $a = 23$ and calculates $A \equiv 2^a \pmod{101}$. Bob chooses a random secret number $b = 39$ and calculates $B \equiv 2^b \pmod{101}$. Alice and Bob exchange A and B . Alice computes $K \equiv B^a \pmod{101}$ and Bob computes $K \equiv A^b \pmod{101}$. The resulting number is their private key, which can be used to communicate securely.
 - (a) Using your calculator, find A , B , and K modulo 101. Why do Bob and Alice get the same private key K ?
 - (b) Suppose that Gary eavesdrops on Alice and Bob's communications. Gary would know what p , g , A and B . Why won't Gary be able to find the private key K ?
 - (c) Is Alice and Bob's secret key safe if they choose $p = 101$? Why or why not? In reality, the prime numbers used are about 300-digits long, which would take the length of the universe to figure out what a is, given p , g , and $A \equiv g^a \pmod{p}$.