Exercise Set 1:
Prime Numbers

Math 414, Winter 2010, University of Washington

Due Wednesday, January 13, 2010

1. Compute $\gcd(2010, 1235)$ by hand.

   Answer: *5*

2. Use the prime sieve describe in the book to find all primes up to 100.

   Answer: *[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]*

3. Prove that there are infinitely many primes of the form $6x - 1$.

   Answer: *Suppose $p_1, \ldots, p_n$ are all the primes of the form $6x - 1$. Let $N = 6p_1 \ldots p_n - 1$. Note that $p_i \nmid N$ for all i. Also note that 2 and 3 do not divide N. The primes ≥ 5 are of the form $6x - 1$ or $6x + 1$ since none of $6x + 2$, $6x + 3$, and $6x + 4$ can be a prime ≥ 5. If every divisor of N is of the form $6x + 1$, then N is also of the form $6x + 1$. This is a contradiction since N is of the form $6x - 1$.*

4. (a) So far 47 Mersenne primes $2^p - 1$ have been discovered. Give a guess, backed up by an argument, about when the next Mersenne prime might be discovered. You will have to do some online research to find the dates when Mersenne primes have been discovered in the past.

   Answer: *Within a year or two, since a plot of nth prime versus year of discover looks roughly linear.*

   (b) EFF will award $150,000 to the first individual or group who discovers a prime with at least 100 million digits (it will very likely be a Mersenne prime). Based on your answer to the first part of this problem, do you think you are likely to see the discovery of a 100 million digit Mersenne prime?

Answer: *A linear model suggests that a 100-digit prime will be found around the end of this century, so I'm unlikely to see this happen (since I'll be well over 100). Note: Many students said in their solutions that they thought powerful quantum computers would be built by then and that these computers would be able to find Mersenne primes quickly. I do* **not** *think a quantum computer would necessarily help at all in finding Mersenne primes. I also doubt that really powerful quantum computers will ever be built.*

5. Let a, b, c, n be integers. Prove that

   (a) if $a \mid n$ and $b \mid n$ with $\gcd(a, b) = 1$, then $ab \mid n$.

   Answer: *Factor a, b and n and note that the factors of a and b are a disjoint set.*

   (b) if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

   Answer: *Easy to see by factoring a, b, c into prime factors.*

6. Let a, b, c, d, and m be integers. Prove that

   (a) if $a \mid b$ and $b \mid c$ then $a \mid c$.

   Answer: *We have integers x, y such that $ax = b$ and $by = c$, so $axy = c$, hence $a \mid c$.*

   (b) if $a \mid b$ and $c \mid d$ then $ac \mid bd$.

   Answer: *We have integers x, y such that $ax = b$ and $cy = d$, so $acxy = bd$, hence $ac \mid bd$.*

   (c) if $m \neq 0$, then $a \mid b$ if and only if $ma \mid mb$.

   Answer: *We have x such that $ax = b$. Hence $max = mb$, so $ma \mid mb$. Conversely, if $max = mb$, then since $m \neq 0$ we have $ax = b$ hence $a \mid b$.*

   (d) if $d \mid a$ and $a \neq 0$, then $|d| \leq |a|$.

   Answer: *We have $dx = a$ with x an integer. Thus $|d| = |a|/|x| \leq |a|$, since $|x| \geq 1$.*

7. (Do this by hand.) Compute the greatest common divisor of $a = 323$ and $b = 437$ using the algorithm described in class that involves quotients and remainders (i.e., do not just factor a and b). Show your work.

   Answer: 19

8. Roughly how long does it take Sage to compute the greatest common divisor of two random 100,000 digit numbers?

   Answer: *about 63 milliseconds:*

```
sage: a = ZZ.random_element(10^(10^5));b = ZZ.random_element(10^(10^5))
sage: timeit('g = gcd(a,b)')
5 loops, best of 3: 63.3 ms per loop
```

9. Suppose that $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ with $a, b, c, d \in \mathbf{Z}$. Prove that one of $a + b\sqrt{-5}$ or $c + d\sqrt{-5}$ is ±1.

   Answer: Write down quadratic polynomial with $a + b\sqrt{-5}, c + d\sqrt{-5}$ as roots, and conclude that if nonreal then they are conjugate. Given this, the result follows easily by multiplying out and equating real and imaginary parts.