Math 312: Problem set 2 (due 19/5/11)

Prime factorization

1. (§3.5.E2) Find the prime factorization of $111,111$.

2. Let $(a,c) = 1$. Show that $(a,bc) = (a,b)$.
   Hint: Factor a,b,c into primes and calculate both sides explicitely.

3. Recall that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.
   (a) Give (with proof) a finite list of primes which contains all prime divisors of $\binom{30}{10}$.
   (b) For each prime on your list, find the number of times it divides $\binom{30}{10}$. Give the prime factorization of this number.

4. We consider the equation $2^x + 3^y = z^2$ for unknown $x,y,z \in \mathbb{Z}_{\geq 0}$.
   (a) (The case $y = 0$) Find all non-negative integral solutions to $2^x + 1 = z^2$.
   Hint: Start by showing that both $z-1$ and $z+1$ must be powers of 2.
   (b) (The case $x = 0$) Find all non-negative integral solutions to $1 + 3^y = z^2$.
   Hint: Which powers of 3 differ by 2?
   (c) Let (x,y,z) be a solution with both of x,y positive and even. Show that $z - 2^{x/2} = 1$.
   Hint: If 3 divides both $z - 2^{x/2}$ and $z + 2^{x/2}$ it would divide their difference.
   (d) Continuing (c), show that $3^y = 2^{1+x/2} + 1$ and find all solutions to this equation.
   Hint: Both $3^{y/2} \pm 1$ must be powers of 2.
   RMK We will show in future problem sets that if (x,y,z) is a solution to the equation above and x,y are positive then x,y are even.

Euclid's Algorithm

5. For each pair of integers a,b use Bezout's extension of Euclid's algorithm to find $\gcd(a,b)$ and integers x,y such that $ax + by = \gcd(a,b)$. Give your intermediate calculations.
   (a) $a = 5$, $b = 2$.
   (b) $a = 60$, $b = 36$.

6. Let $a \geq b \geq 0$.
   (a) Show that $\left(2^a - 1, 2^b - 1\right) = \left(2^a - 1, 2^{a-b} - 1\right)$.
   Hint: Euclid's Lemma + problem 1.
   (b) Show that $\left(2^a - 1, 2^b - 1\right) = 2^{(a,b)} - 1$.
   Hint: Strong induction on $a + b$.
   (c) Show that $\left(x^a - 1, x^b - 1\right) = x^{(a,b)} - 1$ for all $a \geq b \geq 0$ and all $x \geq 2$.

Primes

7. For a positive integer n, show that $n!+1$ has a prime divisor$> n$. Conclude that there are infinitely many primes.

For the next two problems use the identities $x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k}$ and (for n odd) $x^n + y^n = (x+y)\sum_{k=0}^{n-1} (-1)^k x^k y^{n-1-k}$.

8. Let a,n be positive integers such that $a^n - 1$ is prime.
   (a) Show that $a = 2$.
   (b) Show that n is prime.
   Hint: This follows from 6(b) or from the identities above.

8. Let a,b,n be positive integers such that $a^n + b^n$ is prime. Show that n is a power of 2.

Linear equations

9. We study the equation $ax+by=0$ where not both a,b are zero.
   (a) Let a,b be relatively prime. Show that the solutions to $ax+by=0$ are precisely the pairs of the form $x = bz$, $y = -az$ with $z \in \mathbb{Z}$ arbitrary.
   Hint: Note that you both need to verify that these are solutions and to show that every solution is of this form.
   (b) Now let $d = (a,b)$ be anything. Find all solutions to the equation.
   Hint: Divide by d.
   (c) Use part (a) to find all solutions to $5x+6y=1$.
   Hint: $6-5=1$.

Supplementary problems (not for submission): A counting proof of the infinitude of primes

A. In the factorization $n = \prod_p p^{e_p}$ show that $e_p \le \log_2 n$.
B. Assume that $\{p_j\}_{j=1}^{r}$ is the set of all primes, and let $x \ge 2$. Show that there are at most $(1+\log_2 x)^r$ integers between 1 and x.
C. Show that $\frac{(1+\log_2 x)^r}{x} \to 0$ as $x \to \infty$ and derive a contradiction.
D. Use this idea to show that $\pi(x) \ge C\frac{\log_2 x}{\log_2 \log_2 x}$.
E. (unrelated) Let $n = \prod_p p^{e_p} \ge 1$. Show that n has $\tau(n) = \prod_p (e_p+1)$ positive divisors.