Lior Silberman's Math 312: Problem Set 2

Prime factorization

1. Let $a,b\in\mathbb{Z}$ (not both zero) and let $d=\gcd(a,b)$. We show that $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$ in two ways:
   (a) Use Bezout's Theorem to show that there are x,y such that $\frac{a}{d}x+\frac{b}{d}y=1$ and conclude that $\gcd(\frac{a}{d},\frac{b}{d})\mid 1$.
   (b) Express $d,\frac{a}{d},\frac{b}{d}$ using the prime factorizations of a,b and show that $\frac{a}{d},\frac{b}{d}$ have no common prime divisor.

2. Let $(a,c)=1$. Show that $(a,bc)=(a,b)$.
   Hint: Either method of problem 1 works.

3. Consider the equation $2^x+1=z^2$ for unknown $x,z\in\mathbb{Z}_{\geq 0}$.
   (a) Show that $z+1$ and $z-1$ both divide 2^x.
   Hint: rearrange the equation.
   (b) Show that $z+1$ and $z-1$ are both powers of 2.
   (c) Which powers of 2 differ by 2? Use that to solve the equation.

4. Now find all solutions to $1+3^y=z^2$ where $y,z\in\mathbb{Z}_{\geq 0}$.
   Hint: Which powers of 3 differ by 2?

5. We now combine both equations: let $x,y,z\in\mathbb{Z}_{\geq 0}$ solve $2^x+3^y=z^2$. We assume both $x,y>0$ (the cases $y=0$ or $x=0$ are problems 3,4), and we also assume that both x,y are *even*.
   (a) 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.
   (b) Continuing (a), 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

6. Let $a\geq b\geq 0$.
   (a) Show that $\left(2^a-1,2^b-1\right)=\left(2^{a-b}-1,2^b-1\right)$.
   Hint: Euclid's Lemma + problem 2.
   (b) Show that $\left(2^a-1,2^b-1\right)=2^{(a,b)}-1$.
   Hint: Euclid's algorithm
   (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

For the next two problems use the identities

$$\begin{aligned} x^n - y^n &= (x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k} \\ x^{2m+1} + y^{2m+1} &= (x+y)\sum_{k=0}^{2m} (-1)^k x^k y^{2m-k} . \end{aligned}$$

7. Let a, n be integers with $a \geq 1$, $n \geq 2$ 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 ($ab > 1$) such that $a^n + b^n$ is prime. Show that n is a power of 2.
   Hint: Try ruling out $n = 6$ before tackling the general case.

9. (Primes of the form $4k+3$)
   (a) Show that odd numbers have remainder either 1 or 3 when divided by 4.
   (b) Let a, b have remainder 1 when divided by 4. Show that ab has the same reminder.
   Hint: Write $a = 4k+1$, $b = 4\ell+1$ and multiply.
   (c) Suppose a leaves reminder 3 when divided by 4. Show that a is divisible by a prime with the same property.
   (d) Let P be a non-empty set of primes, and let $n = \prod_{p \in P} p$ be their product. Show that no $p \in P$ divides $4n - 1$.
   (e) Show that there are infinitely many primes of the form $p = 4k+3$.

Supplementary problems (not for submission)

A. (A counting proof of the infinitude of primes)
   (a) In the factorization $n = \prod_p p^{e_p}$ show that $e_p \leq \log_2 n$.
   (b) Assume that $\pi(x)$ primes which are at most x. Show that there are at most $(1 + \log_2 x)^{\pi(x)}$ integers between 1 and x.
   (c) There are at least x integers between 1 and x. Conclude that there is a constant C (independent of x) so that
   $$\pi(x) \geq C \frac{\log_2 x}{\log_2 \log_2 x} .$$

B. (unrelated) Let $n = \prod_p p^{e_p} \geq 1$. Show that n has $\tau(n) = \prod_p (e_p + 1)$ positive divisors.