Homework 6 Solutions

Section 3.1

3d) Assume that $3p + 1 = x^2$ for some natural number $x$. Then $3p = x^2 - 1 = (x - 1)(x + 1)$. Now by unique prime factorization since $3$ and $p$ are both primes, then $x - 1 = 3$ or $p$ and $x + 1 = 3$ or $p$. It follows that $x = 4$ and $p = 5$. Thus $p = 5$ is the only prime solution to $3p + 1 = x^2$.

5a) If $p$ is a prime and $p|a^n$, then it must be that $p|n$. Hence $p^n|a^n$.

5b) Assume that $\gcd(a, b) = p$ with $p$ a prime. Then at least one of $a$ and $b$ has exactly one $p$ in its prime factorization. The next three results follow from this fact.

\[
\begin{align*}
gcd(a^2, b^2) &= p^2, \\
gcd(a^2, b) &= p \text{ or } p^2, \\
gcd(a^3, b^2) &= p^2 \text{ or } p^3
\end{align*}
\]

6b) Assume that $n > 4$ is a composite number. Then $n = ab$ with either (1) $1 < a < b < n$ or (2) $1 < a = b < n$. If $1 < a < b < n$, then clearly there is a factor of both $a$ and $b$ in $n - 1!$ and hence $n|(n - 1)!$. In the case $1 < a = b < n$, so $n = a^2$. Since by hypothesis $a > 2$, then $2a \leq n - 1$ and so both $a$ and $2a$ are factors of $n - 1!$ and thus $a^2|n - 1!$. Thus $n|n - 1!$.

7) The prime divisors of 50! are exactly the primes less than 50.

10) Assume that $p \neq 5$ is an odd prime. Then $p = 10n + a$ for some $n \geq 0$ and $a = 1, 3, 7$ or 9. Note that

\[
p^2 = 100n^2 + 20na + a^2 = 10(10n + 2na) + a^2.
\]

If $a = 1$, then we see that $10|p^2 - 1$.

If $a = 3$, then we see that $10|p^2 + 1$.

If $a = 7$, then we see that $10|p^2 + 1$.

If $a = 9$, then we see that $10|p^2 - 1$. 

17) By prime factorization we have that any integer $n$ can be expressed as $n = 2^k \cdot \prod p_i^{e_i}$ where each $p_i$ is an odd prime and $e_i \geq 1$. Now, since each $p_i$ is odd, we have that $\prod p_i^{e_i}$ is an odd integer. Let $m = \prod p_i^{e_i}$, then $n = 2^k m$ where $m$ is an odd integer, as desired.

Section 3.2

2 Use the Sieve to get all primes between 100 and 200. (I’ll leave this one to you. Note that the primes are listed in a table in the back of the book. There is also a Mathematica command for listing them).

4a) This proof is identical to the proof that $\sqrt{2}$ is irrational.

9a) If $n! - 1$ is a prime we are done. So assume $n! - 1$ is composite and has prime divisor $p$. If $p \leq n$, then clearly $p|n!$. But since $p|n! - 1$, we get that $p|1$ a contradiction. Thus $p > n$. Clearly $p < n!$, so are done. □