Homework #3 Solutions

1.5.36. We have $a^3 - a = a(a^2 - 1) = a(a-1)(a+1)$. By the division algorithm, we may write $a = 3k + r$ for some integers k and r with $0 \leq r \leq 2$. If $r = 0$, then $3 \mid a$. If $r = 1$, then $a-1 = 3k+1-1 = 3k$, so $3 \mid a-1$. Finally, if $r = 2$, then $a+1 = 3k+2+1 = 3k+3 = 3(k+1)$, so $3 \mid a+1$. Thus, in each case, 3 divides a factor of $a^3 - a$, and hence divides $a^3 - a$.

3.1.7. Let k be a positive divisor of n with $1 \leq k < n$ (i.e. k is a *proper* positive divisor of n), and write $n = kl$ for some integer l. The identity

$$a^n - 1 = a^{kl} - 1 = (a^k - 1)(a^{k(l-1)} + \cdots + a^k + 1)$$

shows that $a^k - 1$ divides $a^n - 1$. As $a^n - 1$ is prime by assumption, and $a^k - 1 < a^n - 1$ (because $k < n$), we must have $a^k - 1 = 1$. Therefore $a^k = 2$, which implies that $k = 1$ and $a = 2$. Since n is an integer greater than 1 whose only proper positive divisor is 1, we may conclude that n is prime, as desired.

3.1.9. The argument is similar for Euclid's. Suppose there are only finitely many primes. Then there is a positive integer N such that no prime exceeds N. We may assume with no loss of generality that $N \geq 3$. Then $S_N = N! - 1 \geq 3! - 1 = 5 > 1$, so there is a prime p which divides S_N. By hypothesis, $p \leq N$, from which it follows that p divides $N!$, hence that p divides $N! - S_N = 1$, a contradiction. Thus no such N can exist, so there must be infinitely many primes.

3.1.12. The assertion in the statement of the exercise is also valid for $n = 2$, so I am not entirely sure why the restriction $n \geq 3$ is imposed. Whatever dude. Anyway, let $n \geq 2$ and let $Q_n = p_1 \cdots p_{n-1} + 1$. As $n - 1 \geq 1$, $p_1 = 2$ divides $p_1 \cdots p_{n-1}$, so

$$Q_n = p_1 \cdots p_{n-1} + 1 \geq 2 + 1 = 3 > 1.$$

Therefore Q_n has a prime divisor q. If $q = p_i$ for some i with $1 \leq i \leq n-1$, then q divides $p_1 \cdots p_{n-1}$, which implies that q divides $Q_n - p_1 \cdots p_{n-1} = 1$, a contradiction. Thus q is not among the p_i, so $q > p_{n-1}$, from which it follows that $q \geq p_n$. We therefore have $Q_n \geq q \geq p_n$.

3.1.14. Suppose that p is a prime of the form $3n + 1$ for some positive (or nonnegative) integer n. Clearly $p \neq 2$, so p is odd. This implies that n is even, for if n is odd, say $n = 2k + 1$ for some integer k, then

$$p = 3n + 1 = 3(2k + 1) + 1 = 6k + 4 = 2(3k + 2)$$

is even, a contradiction. So we may write $n = 2k$ for some integer k, and thus

$$p = 3n + 1 = 3(2k) + 1 = 6k + 1,$$

so p is also in the second arithmetic progression.

3.1.15. (a) The first prime in the progression $3n + 1$, $n \geq 1$, is 7.
(b) The first prime in the progression $5n + 4$, $n \geq 1$, is 19.
(c) The first prime in the progression $11n + 16$, $n \geq 1$, is 71.

Date: February 7, 2018.

3.1.23. When $n = 2$, n is prime. Assume now that $n \geq 2$ and that for all integers k with $2 \leq k \leq n$, k is either prime or a product of primes. Now consider $n+1$. If $n+1$ is prime, there is nothing else to show, so we may assume $n+1$ is composite. Then we may write $n+1 = ab$ for integers a and b with $1 < a, b < n+1$, i.e., $2 \leq a, b \leq n$. Our inductive hypothesis applied to a and b shows that each is either a prime or a product of primes. It follows that $n+1$ is a product of primes. By induction, the desired assertion holds for all $n \geq 2$.

3.3.6. Let d be the greatest common divisor of a and $a+2$. Then, in particular, d is a common divisor of a and $a+2$, so d also divides $a+2-a = 2$. Therefore $d = 1$ or $d = 2$. If a is even, then $a+2$ is as well, so $d = 2$. If instead a is odd, then $2 \nmid a$, so we must have $d = 1$.

3.3.8. Let a be an even integer, b an odd integer, and $d = (a, b)$. If d is even, then $2 \mid d$, which implies that $2 \mid b$, contradicting the assumption that b is odd. Thus d must be odd.