Homework 2: *1.2*: 3, 7, 8, 10; *1.3*: 2, 6, 7, 8

Exercises 1.2

3. The Fibonacci sequence is defined recursively (inductively) by $a_k = a_{k-1} + a_{k-2}$. Let $P(n)$ be the assertion: a_n and a_{n-1} are relatively prime. Then we see that $a_2 = a_1 = 1$, and so the base case $P(2)$ holds. Now suppose $P(k)$ holds. Using the inductive definition $a_{k+1} = a_k + a_{k-1}$, we see by Lemma 1.1.4 in section 1.1 that $(a_{k+1}, a_k) = (a_k + a_{k-1}, a_k) = (a_{k-1}, a_k)$. But by assumption, $(a_{k-1}, a_k) = 1$, so a_{k+1} and a_k are relatively prime. Thus $P(k) \Rightarrow P(k+1)$, and so by the principle of induction $P(n)$ holds for all $n \in \mathbf{C}$.

7. Let $P(n)$ be the assertion

$$1 + x + x^2 + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x}$$

Then as $\frac{1-x^2}{1-x} = \frac{(1+x)(1-x)}{1-x} = 1 + x$, $P(1)$ holds. Now assume $P(k)$. Then

$$1+x+x^2+\cdots x^n+x^{n+1} = \frac{1 - x^{n+1}}{1 - x} + x^{n+1} = \frac{1 - x^{n+1} + x^{n+1}(1-x)}{1 - x} = \frac{1 - x^{n+2}}{1 - x}$$

Which is the assertion $P(k+1)$. Thus $P(n)$ holds for all n by induction.

8. (i) Proof by induction. $P(n) : 5|n^5 - n$. As $1^5 - 1 = 0 = 5 \cdot 0$, $P(1)$ holds. Now assume $P(k)$. Specifically, say $k^5 - k = 5q$. Then $(k+1)^5 - (k+1) = k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1 = (k^5 - k) + 5(k^4 + 2k^3 + 2k^3 + k) = 5q + 5(k^4 + 2k^3 + 2k^3 + k)$, which is divisible by 5. Thus $P(k+1)$ holds, and so $P(n)$ holds for all n by induction.

(ii) $P(n) : 8|3^{2n} - 1$. Clearly $P(1)$ holds. Now assume $P(k)$. Write $3^{2k} - 1 = 8q$. Then $3^{2k} = 8q + 1$, and so $3^{2(k+1)} - 1 = 3^{2k} \cdot 3^2 - 1 = (8q + 1) \cdot 9 - 1 = 8(9q + 1)$. Thus $8|3^{2(k+1)} - 1$, and so $P(k+1)$ holds. Therefore $P(n)$ holds for all n by induction.

10. We will prove that there cannot be any nonempty set with no least element, which is a restatement of the well-ordering principle. As suggested, let X be an arbitrary set of positive integers with no least element, and define L to be the set of all positive integers n such that n is not greater than or

equal to any element in X. Let $P(n)$ be the assertion $n \in L$. As $1 \leq n$ for every positive integer n, $1 \in L$, and so $P(1)$ holds. Now assume $P(k)$, so $k < x$ for each $x \in X$. But then if $k+1 \notin L$, we must have $k+1 \in X$: there would exist an $x \in X$ such that $x \leq k+1$, but then $k < x \leq k+1$, and so $x = k+1$. Furthermore, $k < x$ for every $x \in X$ implies $k+1 \leq x$ for every $x \in X$, so that $k+1$ would be a least element. As X has no least element this is a contradiction, so we must have $k+1 \in L$. Thus $P(k) \Rightarrow P(k+1)$, and so by induction $P(n)$ holds for all n. But then every n is not in X. In other words, X is empty, and we have proved the well-ordering principle.

Exercises 1.3

2. If n is composite, that is $n = pq$, then we have either $p \leq \sqrt{n}$ or $q \leq \sqrt{n}$ (or both if $n = p^2$). But then using the sieve method n would have been eliminated as a multiple of the smallest prime in the decomposition of n, once primes less than or equal to $\sqrt{n}$ had been accounted for.

6. If n were not prime, say $n = pq$, with $p, q > 1$, then $2^n - 1 = (2^p - 1)(1 + 2^p + 2^{2p} + \cdots + 2^{(q-1)p}$, by polynomial long division (Observe $x = 1$ is a root of $x^q - 1$). But then $2^n - 1$ would be composite. Thus if $2^n - 1$ is not composite, n must be prime.

7. Similarly, if $n = pm$ where $p, m > 0$ and p is an odd prime, then $2^n + 1 = (2^m + 1)(\cdots + 2^{(m-1)p})$, so $2^n + 1$ would be composite.

8. Suppose for contradiction that there were only finitely many primes of the form $4k + 3$. Call them $p_1, p_2, \ldots p_n$. Since $3 = 4 \cdot 0 + 3$ is prime, we may assume $p_1 = 3$. As suggested, let $N = 4(p_2 p_3 \ldots p_n) + 3$. First note that none of the p_i divide N. If N is prime, then we have immediately a contradiction because N is distinct from all of the p_i. Thus, we investigate the case when N is not prime. If this were the case, then as N is not divisible by any of the finitely many primes of the form $4k+3$, N must be a product of primes not of the form $4k+3$. Since 2 does not divide N, we may assume $N = q_1 q_2 q_3 \ldots q_m$ as a product of (not necessarily distinct) primes of the form $4k+1$. But then we note that for each i, $q_i \equiv 1 (\text{mod } 4)$. Thus $N \equiv q_1 \cdots q_m \equiv 1 \cdots 1 \equiv 1(\text{mod } 4)$. Which is a contradiction, as $N \equiv 3(\text{mod } 4)$ by definition. Thus if our list $p_1, \ldots p_n$ were complete, we would be able to construct a number N which is neither prime nor composite, which is of course a contradiction, so our list cannot be complete.