M417 Homework 2 Spring 2004

(1) Let a, b and c be positive integers such that $a|c$ and $b|c$.

(a) If $gcd(a,b) = 1$, prove that $ab|c$: Since $a|c$ and $b|c$, we can write $as = c$ and $bt = c$ for some integers s and t. But we know there exist x and y such that $gcd(a,b) = ax + by$, so we have $1 = ax + by$ and hence $c = c(ax + by) = cax + cby = btax + asby = ab(tx + sy)$, so $ab|c$.

(b) Give a counterexample to the statement: If $(gcd(a,b))^2$ divides c, prove that $ab|c$. Let $a = 12$, $b = 18$ and $c = 36$. Then $gcd(a,b) = 6$, so $(gcd(a,b))^2$ divides c, but $ab = 216$ does not divide c.

(2) Prove that there are infinitely many primes: Suppose there are only finitely many primes. List them: $\{P_1, P_2, \ldots, P_n\}$. Let $P = P_1 P_2 \ldots P_n + 1$. By the Fundamental Theorem of Arithmetic, P is either a prime or a product of primes. In any case, P is divisible by some prime, and hence $P_i|P$ for some i. But in fact none of the primes in the list $\{P_1, P_2, \ldots, P_n\}$ can divide P, since each leaves a remainder of 1. This contradicts there being a finite list of primes. Hence the set of primes is infinite.

(3) # 26, p. 24: We want to prove that $f_n < 2^n$, where $f_1, f_2, \ldots$ is the Fibonacci sequence (defined recursively by $f_1 = 1$, $f_2 = 1$, and $f_{k+1} = f_k + f_{k-1}$ for each $k \geq 2$). Clearly $f_n < 2^n$ holds for $n = 1$ and $n = 2$. Now suppose $n > 2$ and that $f_k < 2^k$ holds for all $1 \leq k < n$. Then $f_n = f_{n-1} + f_{n-2} < 2^{n-1} + 2^{n-2} < 2^{n-1} + 2^{n-1} = 2(2^{n-1}) = 2^n$. By induction, this shows that $f_n < 2^n$ holds for all positive integers n.

(4) Let R be the relation on the set of integers defined by aRb exactly when $a - b$ is odd. Determine with justification whether or not R is: reflexive; symmetric; transitive. Answer: First, R is not reflexive, since aRa holds exactly when $a - a$ is odd, but $a - a$ is always even. Nor is R transitive, since if aRb and bRc hold, then $a - b$ and $b - c$ are odd, hence $a - c = (a - b) + (b - c)$ is even, so aRc does not hold. But R is symmetric, since if aRb holds, then $a - b$ is odd, hence $b - a = -(a - b)$ is odd too, so bRa holds.

(5) Answer: For me, the string is 011, so I must find a relation R on a set S which is not reflexive, but which is symmetric and transitive. Let R be any relation which is symmetric and transitive. If there are any two related elements of S, say aRb, then bRa by symmetry and hence aRa by transitivity. For R to fail to be reflexive, there must be some element $a \in S$ such that aRa fails to hold. By what we just saw, a thus cannot be related to *any* element of S. So let S be any nonempty set and take R to be empty; i.e., no element is related to any element. Then R is not reflexive (since S is nonempty, there is some $a \in S$ for which aRa fails), but R is symmetric (since whenever aRb holds—which is never—we always have bRa) and transitive (since whenever aRb and aRc hold, we always have aRc).