MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL TERM 2024, SOLUTIONS 5

1. Let $\{F_n : n = 0, 1, \dots\}$ be the Fibonacci sequence defined by $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$ and let

$$\theta = \frac{1+\sqrt{5}}{2} = 1.6180339887498948482045868343656\dots.$$

(i) Prove that $F_n = \frac{\theta^n - (-\theta)^{-n}}{\sqrt{5}}$. (ii) Suppose that a and b are positive integers with $b \le a$ and we adopt the notation used in the description of Euclid's algorithm. Prove that for $k = 0, 1, \dots, s-1$ we have $F_k \le r_{s-1-k}$ and $s \le 1 + \frac{\log 2b\sqrt{5}}{\log\theta}$.

(i) θ and $\phi = -1/\theta = (1-\sqrt{5})/2$ are both solutions to $x^2 - x - 1 = 0$ and hence to $x^{n+1} = x^n + x^{n-1}$. Moreover (i) holds for $n = 0$ and 1 and hence by induction for all n. (ii) $r_{s-1} \ge 1 \ge 0 = F_0$ and $r_{s-2} \ge 1 = F_1$. Suppose that $2 \le k \le s-1$ and $F_j \le r_{s-1-j}$ holds for $0 \le j \le k-1$. Then $r_{s-1-k} = r_{s-1-(k-1)}q_{s-k+1} + r_{s-1-(k-2)} \ge r_{s-1-(k-1)} + r_{s-1-(k-2)} \ge F_{k-1} + F_{k-2}$, so by induction on k, $r_{s-1-k} \ge F_k$. Let $k = s-1$. Then $F_{s-1} \le r_0 = b$ and the desired inequality follows by taking logs and applying the formula for F_{s-1}.

2. Solve where possible. (i) $91x \equiv 84 \pmod{143}$. (ii) $91x \equiv 84 \pmod{147}$

(i) $13|(143, 91$, but $13 \nmid 84$, so insoluble. (ii) $(91, 147) = 7|84$, so 7 solutions, $x \equiv 9, 30, 51, 72, 93, 114, 135 \pmod{147}$.

3. Prove that $7n^3 - 1$ can never be a perfect square.

A perfect square always leaves one of the remainders $0, 1, 2, 4$ on division by 7, never the remainder $6 \equiv -1$.

4. Suppose that $m_1, m_2 \in \mathbb{N}$, $(m_1, m_2) = 1$, $a, b \in \mathbb{Z}$. Prove that $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$ if and only if $a \equiv b \pmod{m_1 m_2}$.

If $a \equiv b \pmod{m_1 m_2}$, then $m_1 m_2 | b - a$, so each of m_j divides $b - a$. If $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$, so that $m_1 | b - a$ and $m_2 | b - a$, then since m_1 and m_2 have no prime factors in common we have $m_1 m_2 | b - a$.

5. Solve the simultaneous congruences $x \equiv 3 \pmod 6, x \equiv 5 \pmod{35}, x \equiv 7 \pmod{143}, x \equiv 11 \pmod{323}$.

The general solution is given by $x \equiv 3m_1n_1 + 5m_2n_2 + 7m_3n_3 + 11m_4n_4 \pmod m$ where $m = 6.35.143.323 = 9699690$, $m_1 = m/6 = 1616615 \equiv 5 \pmod 6$, $m_2 = m/35 = 277134 \equiv 4 \pmod{35}$, $m_3 = m/143 = 67830 \equiv 48 \pmod{143}$, $m_4 = m/323 = 30030 \equiv 314 \pmod{323}$, $m_1n_1 \equiv 1 \pmod 6$, $m_2n_2 \equiv 1 \pmod{35}$, $m_3n_3 \equiv 1 \pmod{143}$, $m_4n_4 \equiv 1 \pmod{323}$. Thus $n_1 = 5$, $n_2 = 9$, $n_3 = 3$, $n_4 = 287$ and $x \equiv 3.1616615.5 + 5.277134.9 + 7.67830.3 + 11.30030.287 = 132949395 \equiv 6853425 \pmod{9699690}$.