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

Return by Monday 30th September

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

$$s \le 1 + \frac{\log 2b\sqrt{5}}{\log \theta}.$$

This shows that Euclid's algorithm runs in time at most linear in the bit size of $\min(a, b)$.

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

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

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 $a \equiv b \pmod{m_1 m_2}$.

5. Solve the simultaneous congruences

$$\begin{aligned} x &\equiv 3 \pmod{6} \\ x &\equiv 5 \pmod{35} \\ x &\equiv 7 \pmod{143} \\ x &\equiv 11 \pmod{323} \end{aligned}$$