HOLIDAY PROBLEMS, MP313, Semester 2, 1999.

1. Let p be an odd prime. Use Thue's theorem to prove that p is expressible as $x^2 - 2y^2$ if and only if $p \equiv \pm 1 \pmod{8}$. (Hint: The identity

$$(x+2y)^2 - 2(x+y)^2 = 2y^2 - x^2$$

will be useful.)

2. Verify all the recurrence relations that preceded the Lucas–Lehmer primality test.

3. Let p be an odd prime.

   (a) If $p-1 = 2^s t$, where t is odd, prove that the number of integers x in $1 \le x \le p-1$ for which $\mathrm{ord}_p x$ is even is equal to $(p-1)(1-1/2^s)$.

   (b) Let $p \equiv 3 \pmod{4}$, p not dividing x. Prove that $\mathrm{ord}_p x$ is even if and only if $\left(\frac{x}{p}\right) = -1$.

4. (**) Let $p \equiv 1 \pmod{4}$ be a prime, p not dividing k and let

$$S(k) = \sum_{x=1}^{p-1} \left(\frac{x(x^2+k)}{p}\right).$$

   (a) Prove that $S(k)$ is even.

   (b) Verify that $S(kt^2) = \left(\frac{t}{p}\right) S(k)$ if p does not divide k.

   (c) By expanding $\displaystyle\sum_{k=1}^{p-1} (S(k))^2$ in two ways, use Question 8 of Sheet 4 to deduce that

$$p = (S(r))^2 + (S(n))^2,$$

   where r and n are any quadratic residues, nonresidues, respectively. (eg. r can be taken to be ± 1.)

   (d) Show that $\displaystyle\frac{S(-1)}{2} = \sum_{x=1}^{\frac{p-1}{2}} \left(\frac{x(x^2-1)}{p}\right)$ is odd.

   (e) Show that $S(1) \equiv -\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod{p}$ by using Euler's criterion.

(f) Deduce that $p = x^2 + 1$ for some $x \in \mathbb{N}$ if and only if

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \pm 2 \pmod{p}.$$

5. Verify that $\frac{7+5\sqrt{2}}{3}$ is reduced and that

(a) $\frac{7+5\sqrt{2}}{3} = [\overline{4, 1, 2, 4, 2, 1, 4, 42}]$;

(b) $21 + 15\sqrt{2} = [\overline{42, 4, 1, 2, 4, 2, 1, 4}]$.

6. Suppose $x \in \mathbb{Q},\ x \notin \mathbb{Z}$. Prove that

$$\left\lfloor \frac{x}{m} \right\rfloor = \begin{cases} \left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor & \text{if } m \in \mathbb{N}, \\ \\ \left\lfloor \frac{1+\lfloor x \rfloor}{m} \right\rfloor & \text{if } m \in -\mathbb{N}. \end{cases}$$