MA1301 TALLTEORI

20. XII. 2006

Peter Lindqvist

---

(1) $10m^2 = n^2$. We may assume that
$\gcd(m,n) = 1$.

$10m^2 = n^2 \Rightarrow 2 \mid n^2 \Rightarrow 2 \mid n$

Thus $n = 2k$ and so

$10m^2 = 4k^2 \Rightarrow 5m^2 = 2k^2 \Rightarrow 2 \mid m^2$

$\Rightarrow 2 \mid m$

We get the contradiction $\gcd(m,n) \geq 2$.
It follows that $\sqrt{10}$ is irrational.

---

(2) $\varphi(1000) = 400$, $7^{400} \equiv 1 \pmod{1000}$ by the Euler–Fermat theorem. Thus

$2007^{2006} \equiv 7^{2006} \equiv 7^{5\cdot 400 + 6} \equiv (7^{400})^5 7^6$

$\equiv 1^5 7^6 \equiv 7^6 \equiv 649 \pmod{1000}$. The three last digits are $\underline{\underline{649}}$.

---

(3) $$\begin{cases} x \equiv 2 \pmod 3 \\ 2x \equiv 3 \pmod 5 \\ 3x \equiv 4 \pmod 7 \end{cases}$$

In order to use the Chinese Remainder Thm in the version given in the book, we avoid the factors 2 and 3:

$2x \equiv 3 \pmod 5 \Leftrightarrow -3x \equiv 3 \Leftrightarrow x \equiv -1 \pmod 5$

$3x \equiv 4 \pmod 7 \Leftrightarrow -4x \equiv 4 \Leftrightarrow x \equiv -1 \pmod 7$

continues

Thus the system is equivalent to

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv -1 \pmod 5 \\ x \equiv -1 \pmod 7 \end{cases}$$

The moduli 3, 5, 7 are pairwise prime. By the Chinese Remainder Theorem the solution is unique modulo $3 \cdot 5 \cdot 7 = 105$. We solve the auxiliary equations (they are independent)

$$35 x_1 \equiv 1 \pmod 3, \qquad x_1 = -1$$
$$21 x_2 \equiv 1 \pmod 5, \qquad x_2 = 1$$
$$15 x_3 \equiv 1 \pmod 7, \qquad x_3 = 1$$

Hence

$$x = 35 \cdot (-1) \cdot 2 + 21 \cdot 1 \cdot (-1) + 15 \cdot (1) \cdot (-1)$$
$$= -106 \equiv -1 \equiv 104 \pmod{105}$$

<u>Answer</u>: $\underline{104 + 105n}$, $n = 0, \pm 1, \pm 2, \ldots$

---

(4)

$$\boxed{x^2 - 33y^2 = 1}$$

0	1	2	3	4
5	1	2	1	10
5	6	17	23	
1	1	3	4	

$p_3 = 23$

$q_3 = 4$

Since the period is of length 4, the fundamental solution is $x = p_3 = \underline{23}$, $y = q_3 = \underline{4}$. Now

$$x_2 + y_2\sqrt{33} = (23 + 4\sqrt{33})^2$$

yields the solution $x = \underline{\underline{1057}}$, $y = \underline{\underline{184}}$.

48599, 8460; 2234497, 388976.

(5) $x^{37} \equiv 12 \pmod{55}$ $\quad x = ?$

$$\varphi(55) = (5-1)(11-1) = 40$$

From $37d \equiv 1 \pmod{40}$ we obtain

$$d = 13 \quad \text{(decryption key).}$$

This comes from $37d + 40y = 1$, when the Euclidean algorithm is used. Finally,

$$x = 12^{13} \equiv 12 \pmod{55}.$$

(Explanation: $12^{13} = (x^{37})^{13} = x^{37\cdot 13} = x^{1+40k}$

$= (x^{40})^k x \equiv 1^k x \equiv x \pmod{55}$ because

$x^{40} \equiv 1 \pmod{55}$ Euler-Fermat.)

---

(6) It is understood that $n \geq 2$, $a > 0$.

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

This is a factorization, except for $a - 1 = 1$, i.e., $a = 2$. Therefore $a^n - 1$ is not a prime when $a \neq 2$, $n \geq 2$.

Now

$$2^{jk} - 1 = (2^j)^k - 1$$

To avoid factorization one must again have $2^j = 2$ $(= a)$ so that $j = 1$. Remark: This leads to the Mersenne primes

$$2^p - 1.$$

(7) $111\cdots11 = 111\cdots100 + 11$

$= 4k' + 11 = 4k + 3$

A square cannot be of the type $4k+3$, because we have only the cases

$$(2n)^2 = 4n^2 = \text{"}4k\text{"}$$

$$(2n+1)^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1 = \text{"}4k+1\text{"}.$$

Hence $111\cdots11$ is never a square (except $1 = 1^2$).