ELEMENTARY NUMBER THEORY

HOMEWORK 7

(1) Let

$$a = 1 + 3 \cdot 5 + 4 \cdot 5^2 + \ldots,$$
$$b = 3 + 2 \cdot 5 + 2 \cdot 5^2 + \ldots$$

Compute approximations modulo 5^2 for $a+b$, $a-b$, ab and a/b.

we get

$$\begin{aligned} a + b &= 4 + 5 \cdot 5 + 6 \cdot 5^2 + \ldots \\ &= 4 + 0 \cdot 5 + 7 \cdot 5^2 + \ldots \\ &= 4 + 0 \cdot 5 + 2 \cdot 5^2 + \ldots, \\ a - b &= -2 + 1 \cdot 5 + 2 \cdot 5^2 + \ldots \\ &= 3 + 0 \cdot 5 + 2 \cdot 5^2 + \ldots, \\ ab &= 3 + 11 \cdot 5 + 20 \cdot 5^2 + \ldots \\ &= 3 + 1 \cdot 5 + 22 \cdot 5^2 + \ldots \\ &= 3 + 1 \cdot 5 + 2 \cdot 5^2 + \ldots \end{aligned}$$

For computing $c = a/b$, we write

$$\begin{aligned} 1 + 3 \cdot 5 + 4 \cdot 5^2 + \ldots &= (3 + 2 \cdot 5 + 2 \cdot 5^2 + \ldots)(c_0 + c_1 \cdot 5 + c_2 \cdot 5^2 + \ldots) \\ &= 3c_0 + (3c_1 + 2c_0) \cdot 5 + (3c_2 + 2c_1 + 4c_0) \cdot 5^2 + \ldots \end{aligned}$$

Reducing this equation modulo 5 gives $3c_0 \equiv 1 \bmod 5$, hence $c_0 = 2$. Reduction modulo 5^2 then shows that $1 + 3 \cdot 5 \equiv 6 + (3c_1 + 2 \cdot 2) \cdot 5 \bmod 5^2$, hence $16 \equiv 26 + 15c_1 \bmod 5^2$; this is equivalent to $3c_1 \equiv -2 \bmod 5$, and this gives $c_1 = 1$.

Finally, reduction modulo 5^2 now gives $1 + 3 \cdot 5 + 4 \cdot 5^2 \equiv 6 + 7 \cdot 5 + (3c_2 + 2 + 8) \cdot 5^2 \bmod 5^3$, which leads to $116 \equiv 291 + 75c_2 \bmod 5^3$ and $0 \equiv 7 + 3c_2 \bmod 5$. This gives $c_2 = 1$, hence $a/b = 2 + 1 \cdot 5 + 1 \cdot 5^2 + \ldots$.

(2) Show that $\sqrt{2} \in \mathbb{Z}_{17}$.

(a) First solve $x_1^2 \equiv 2 \bmod 17$.
$2 \equiv 19 \equiv 36 \equiv 6^2 \bmod 17$, hence $x_1 = 6$.

(b) Write $x_2 = x_1 + 17y$ and determine $y \bmod 17$ in such a way that $x_2^2 \equiv 2 \bmod 17^2$.
Let $x_2 = 6 + 17y$; then $2 \equiv x_2^2 \equiv 36 + 12y \cdot 17 \bmod 17^2$ shows that $17^2 \mid (34 + 12y \cdot 17$, i.e., that $17 \mid 2 + 12y$. This gives $y \equiv -3 \bmod 17$, and we have $x_2 = 6 + 14 \cdot 17$.

(c) Prove by induction that you can solve $x_k^2 \equiv 2 \bmod 17^k$ for every $k \geq 1$.
Assume that $x_k = 6+14\cdot 17+\ldots+y_{k-1}17^{k-1}$ satisfies $x_k^2 \equiv 2 \bmod 17^k$. Then write $x_{k+1} = x_k + y_k 17^k$; using the fact that $x_k^2 = 2 + 17^k a$ for some integer a we find

$$2 \equiv x_{k+1}^2 \equiv x_k^2 + 2x_k y_k 17^k = 2 + 17^k a + 2x_k y_k 17^k \bmod 17^{k+1}.$$

Thus we have to pick y_k in such a way that $a + 2x_k y_k \equiv 0 \bmod 17$. This can be done if and only if $2x_k$ has an inverse modulo 17, that is, if and only if $17 \nmid x_k$, which is the case since $x_k \equiv 6 \bmod 17$.

(d) Prove that the sequence x_k is a Cauchy sequence with respect to $|\cdot|_{17}$.
For $m > n$ we have $x_m - x_n = y_n \cdot 17^n + \ldots + y_{m-1} \cdot 17^{m-1}$, hence $|x_m - x_n|_{17} \leq 17^{-n}$. Thus $|x_m - x_n|_{17}$ can be made as small as we wish by picking n large enough.

(e) Let x be the 17-adic number defined by the Cauchy sequence x_k. Show that $x^2 = 2$.
Let $x = \lim_k x_k = 6 + 4 \cdot 17 + \ldots$ be the 17-adic integer defined by the sequence of the x_k. We know that $x \equiv x_k \bmod 17^k$ for all $k \geq 1$, hence $x^2 \equiv x_k^2 \equiv 2 \bmod 17^k$. This shows that $17^k \mid (x^2 - 2)$ for all $k \geq 1$. If $x^2 - 2 \neq 0$, then $x^2 - 2 = 17^m u$ for some integer m and some 17-adic unit u; but then $17^k \mid 17^m u$ is false for $k > m$, and this contradiction proves that $x^2 - 2 = 0$.

(3) Show that the equation $x^3 = 2$ has no solution in $\mathbb{Z}_7$.

Assume that $x = a+7b+7^2c+\ldots$ with $0 \leq a, b, c, \ldots < 7$, satisfies $x^3 = 2$. Since $x \equiv a \bmod 7$ we find $2 = x^3 \equiv a^3 \bmod 7$. But $a^3 \equiv 0, \pm 1 \bmod 7$, hence there is no such a (and therefore no such x).