Вокруг p-адических чисел

Как известно, целые числа в компьютере - не целые числа вовсе, а скорее остатки от деления на 2^n. Для таких чисел было бы интересно научиться решать уравнения быстрее чем полным перебором. Это можно делать итерационно. Пускай для некоторого многочлена f мы хотим решить сравнение $f(x) = 0 \pmod{2^n}$ и при этом мы уже нашли решение b_k по меньшему модулю 2^k. Тогда решение по модулю 2^{k+1} можно искать в виде $b_{k+1} = b_k + a_k 2^k$ где $a_k \in \{0, 1\}$. Как правило, из соотношения $f(b_k + a_k 2^k) = 0 \pmod{2^{k+1}}$ цифра a_k находится однозначно.

Упражнение 1. а) Возьмите для определённости целочисленный тип данных uint32_t (беззнаковый 32х битный тип) и с помошью описанного метода найдите все корни третьей степени из единицы. Иначе говоря, решите сравнение $x^3 = 1 \pmod{2^{32}}$.
б) Для типа uint8_t извлеките квадратный корень из 17, т.е. решите $x^2 = 17 \pmod{2^8}$.
в*) Попытайтесь заполнить пробелы в описании данного метода, докажите, что он находит все решения, опишите его границы применимости.

Итак, описанный алгоритм позволяет строить последовательность решений некоего уравнения по модулям вида p^k, постепенно уточняя старшие цифры. Но почему мы должны останавливаться при $k = 8$ или $k = 32$? Почему бы не продолжить эту последовательность дальше?

Определение. Зафиксируем простое p. Целым p-адическим числом $z \in \mathbb{Z}_p$ называется:

1. Последовательность $z = (b_1, b_2, b_3, \dots)$ где $b_k \in \mathbb{Z}/p^k\mathbb{Z}$ и для $i > j$ выполнено $b_i \pmod{p^j} = b_j$. Операции при этом выполняются покомпонентно.
2. Формальный степенной ряд $z = \sum\limits_{n=0}^{\infty} a_n p^n$ где $a_k \in \mathbb{Z}/p\mathbb{Z}$. Операции над такими рядами выполняются “в столбик” по стандартным правилам арифметики.

Упражнение 2. а) Докажите эквивалентность двух определений.
б) Найдите p-адическую запись -1. Сравните с представлением -1 в компьютере.
в) Чем особенна p-адическая запись (обыкновенного) целого числа?
г) Покажите, что $\mathbb{Z}_p$ (целые p-адические числа) образуют кольцо.
д) Какие элементы $\mathbb{Z}_p$ не являются обратимыми?

Определение. По аналогии с построением рациональных чисел определим $\mathbb{Q}_p$ (рациональные p-адические числа) как множество формальных дробей вида $\frac{z_1}{z_2}$ где $z_1, z_2 \in \mathbb{Z}_p$ и $z_2 \neq 0$ с отождествлением $\frac{z_1}{z_2} = \frac{w_1}{w_2} \iff z_1 w_2 = w_1 z_2$. Операции определяются следующим образом: $\frac{z_1}{z_2} + \frac{w_1}{w_2} = \frac{z_1 w_2 + w_1 z_2}{z_2 w_2}$ и $\frac{z_1}{z_2} \times \frac{w_1}{w_2} = \frac{z_1 w_1}{z_2 w_2}$.

Упражнение 3. а) Покажите что операции определены корректно
б) Покажите что $\mathbb{Q}_p$ является полем и содержит $\mathbb{Q}$
в) Покажите что любое $q \in \mathbb{Q}_p$ можно представить в виде $q = \sum\limits_{n=n_0}^{\infty} a_n p^n$ где $n_0 \in \mathbb{Z}$.
г) Чем особенна p-адическая запись (обыкновенного) рационального числа?
д) Является ли поле $\mathbb{Q}_p$ алгебраически замкнутым?

Определение. Пусть $q \in \mathbb{Q}_p$ и $q = \sum\limits_{n=n_0}^{\infty} a_n p^n$ и $a_{n_0} \neq 0$. Тогда p-адической нормой q называется величина $|q|_p = p^{-n_0}$. При $q = 0$ по определению считают $|q|_p = 0$.

Для $x, y \in \mathbb{Q}_p$ p-адическим расстоянием между x и y называют $d_p(x, y) = |x - y|_p$.

Упражнение 4. а) Какие числа "ближе" относительно d_3 — 1 и $\frac{7}{9}$ или 1 и 46?
б) Докажите усиленное неравенство треугольника: $d_p(x, z) \leq \max\{d_p(x, y), d_p(y, z)\}$.
в) Проверьте что функции $|\_|_p$ и $d_p(\_, \_)$ являются нормой и метрикой на $\mathbb{Q}_p$.
г) Является ли метрическое пространство $(\mathbb{Q}_p, d_p)$ полным?
д) $\mathbb{Z}_2$ гомеоморфно Канторовому множеству. Что можно сказать про $\mathbb{Z}_p$, $\mathbb{Q}_p$?

Упражнение 5. Пространства, в которых выполнено усиленное неравенство треугольника, называют неархимедовыми. Согласно пункту 4б поле $\mathbb{Q}_p$ — неархимедово.
а) В неархимедовом пространстве любой треугольник равнобедренный.
б) В неархимедовом пространстве любая точка шара является его центром.
в) В неархимедовом пространстве из двух шаров имеющих общую точку один обязательно содержится в другом.
г) В $(\mathbb{Q}_p, d_p)$ любой открытый шар замкнут.

Определение. Предел последовательности и сумма ряда определяются как и в $\mathbb{R}$.

Упражнение 6 ("мечта студента"). Пусть $q_n \in \mathbb{Q}_p$ — произвольная последовательность чисел. Покажите что ряд $\sum\limits_{n=0}^{\infty} q_n$ сходится если и только если $|q_n|_p \xrightarrow{n\to\infty} 0$.

Упражнение 7. Каков радиус сходимости следующих рядов и что можно сказать про сходимость на границе? Ответы могут отличаться при $p = 2$ и $p > 2$.

а) $L(x) = -\ln(1 - x) = \sum\limits_{n=1}^{\infty} \frac{x^n}{n}$ б) $\exp(x) = \sum\limits_{n=0}^{\infty} \frac{x^n}{n!}$

Мы приближаемся к основной цели данного листочка — вычислению группы обратимых элементов $(\mathbb{Z}/n\mathbb{Z})^\times$. Доказательства элементарными методами известны, но оставляют желать лучшего. Китайская теорема об остатках учит нас, что достаточно решить задачу для $n = p^k$.

Упражнение 8. а) Любое число $x \in \mathbb{R}^\times$ однозначно представляется в виде $x = \pm e^s$ где $s \in \mathbb{R}$. Осознайте, что это влечёт изоморфизм $\mathbb{R}^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{R}$.
б) Найдите $\mathbb{Q}^\times$, $\mathbb{C}^\times$. Выразите $\mathbb{Q}_p^\times$ через $\mathbb{Z}_p^\times$.
в*) Установите изоморфизм. <Hint: вам может пригодиться функция $L(x)$>

$$\mathbb{Z}_2^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}_2$$
$$\mathbb{Z}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p \text{ при } p > 2$$

Упражнение 9. а*) Выведите из 8в следующие изоморфизмы:

$$(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{k-2}\mathbb{Z}$$
$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/p^{k-1}\mathbb{Z} \text{ при } p > 2$$

б) Первообразные корни существуют только по модулям $n = 2, 4, p^\alpha, 2p^\alpha$ где $p > 2$.