List 6 : Hensel lifting

Manuel Loeda

Exercise 7 // Let $N = pq$ be the product of two distinct primes p and q.

i) $u \equiv p^2 \bmod q$ and $u \equiv q^2 \bmod p$, thus, by Chinese Remainder Theorem, it is a unit modulo pq.

ii) Verify the factorization $x \equiv u^{-1}(px+q)(qx+p) \bmod N$

$$(px+q)(qx+p) = pqx^2 + q^2x + pq + p^2x \equiv ux \bmod N \Rightarrow$$

$$x = u^{-1}(px+q)(qx+p)$$

iii) $g, h \in \mathbb{Z}[x]$ with $px+q \equiv gh \bmod pq$.

$q \equiv gh \bmod p \Rightarrow g, h$ are units modulo p.

$px \equiv gh \bmod q \Rightarrow g$ or h irreducible modulo q

C.R.T $\Rightarrow$ ~~∄~~ g or h unit modulo pq. $px+q$ irreducible modulo pq.

Exercise 9 // Let R be a commutative ring, and f and $g \in R[x]$, with g nonzero and monic.

a) Show that there exist unique polynomials $q, r \in R[x]$ with $f = qg + r$ and either $r = 0$ or $\deg r < \deg g$.

Proof: Division with remainder algorithm.

b) If $f \equiv 0 \pmod m$ for some $m \in R$, then show that $q \equiv r \equiv 0 \pmod m$.

$f = mp \quad p \in R[x]$

by a) $p = q'g + r' \quad q', r' \in R[x] \quad \deg r' < \deg g$

$$\left.\begin{array}{l} f = mp = (mq')g + mr' \\ f = \quad\quad qg + r \end{array}\right\} \Rightarrow \text{by uniqueness of div with remainder } q = mq', \quad r = mr'$$

$$\Downarrow \qquad \Downarrow$$

$$q \equiv 0 \pmod m \quad r \equiv 0 \pmod m.$$

~~Exercise 3 $f: x^3 - 292x^3 - 2170221x + 66568000 \in \mathbb{Z}[x]$ 13-adic linear factors $x - a_i$ with $f \equiv \prod(x-a_i) \equiv 0 \bmod 13^2$ $i = 0,1,2$ $a_0 \neq 0$. Using Mathematica for computations~~

Exercise 3: $f: x^3 - 292x^3 - 2170221 + 66560000 \in \mathbb{Z}[x]$ 13-adic linear factors $x - a_i$ with $f \equiv \prod(x-a_i) \equiv 0 \bmod 13^{2^i}$ $i = 0,1,2$. Starting from $a_0 = 0$. By it of the Hensel step and with the help of mathematica

$$a_0 = 0, \; a_1 = 65, \; a_2 = 1625.$$