Manuel Kauers
RISC-Linz

Hagenberg, December 2, 2002

Computer Algebra Exercises
Solution 5

Ex. (21) We compute the gcd of

$$a = x^4 - x^3 - 2x^2 + 3x - 1 \quad \text{and}$$
$$b = x^4 - x^3 + x^2 + x - 2$$

using the modular algorithm. In our case, $d = \gcd(\mathrm{lc}(a), \mathrm{lc}(b)) = 1$ and

$$\begin{aligned} M &= 2 \cdot 2^{\min(4,4)} \gcd(a_4, b_4) \cdot \min\left(\frac{1}{|a_4|}\sqrt{\sum_{i=0}^{4} a_i^2}, \frac{1}{|b_4|}\sqrt{\sum_{i=0}^{4} b_i^2}\right) \\ &= 2 \cdot 2^4 \cdot 1 \cdot \min(\sqrt{16}, \sqrt{8}) \\ &= 64\sqrt{2}. \end{aligned}$$

By $x_{(p)}$ we denote $x \bmod p$, and we write

$$g_{(p)} = c_{(p)} = \gcd(a_{(p)}, b_{(p)})$$

(Note that $d_{(p)} = d = 1$ in our special case.) The steps of the computation can be read from the following table.

P	p	$f_{(p)}$, $g_{(p)}$	$g_{(p)}$	g
1	2	$x^4 + x^3 + x + 1$ $x^4 + x^3 + x^2 + x$	$x^2 + 1$	$x^2 + 1$
2	3	$x^4 + 2x^3 + x^2 + 2$ $x^4 + 2x^3 + x^2 + x + 1$	$2x + 1$	$\lightning$
1	5	$x^4 + 4x^3 + 3x^2 + 3x + 4$ $x^4 + 4x^3 + x^2 + x + 3$	$2x + 3$	$2x - 2$
5	7	$x^4 + 6x^3 + 5x^2 + 3x + 6$ $x^4 + 6x^3 + x^2 + x + 5$	$5x + 2$	$12x - 12$
35	11	$x^4 + 10x^3 + 9x^2 + 3x + 10$ $x^4 + 10x^3 + x^2 + x + 9$	$8x^2 + 2x + 1$	$12x - 12$
385				

Finally, since $P = 385 > 64\sqrt{2}$ we are done with the loop, so we redefine g to its primitive part:

$$g = \mathrm{pp}(12x - 12) = x - 1.$$

We check by

$$a/g = x^3 - 2x + 1, \qquad b/g = x^3 + x + 2$$

that g is actually a divisor.

The polynomial remainder sequence approach is actually also not too bad on this particular example:

$$\begin{aligned}
&x^4 - x^3 - 2x^2 + 3x - 1\\
&x^4 - x^3 + x^2 + x - 2\\
&-3x^2 + 2x + 1\\
&132x - 132\\
&0.
\end{aligned}$$

Ex. (22)

Ex. (23) Given a prime p and $m \in \mathbb{N}$, let $K = \mathrm{GF}(p)$, $L = \mathrm{GF}(p^m) = K(\alpha)$, $q = p^m$ and

$$f = \sum_{i=0}^{q-1} a_i x^i \in L[x].$$

We are about to show the equivalence of

1. $\forall a \in L : f(a) \in K$ and
2. $x^q - x \mid f(x)^p - f(x)$.

We first prove the equivalence of $x^p = x$ and $x \in K$ as a lemma. The direction from right to left is asserted by Fermat. As for the other direction, take an arbitrary $x = \alpha^k \in L$. Then

$$\begin{aligned}
& \alpha^k = (\alpha^k)^p = \alpha^{kp}\\
\Longrightarrow\quad & k = kp \bmod q\\
\Longrightarrow\quad & k(p-1) = 0 \bmod q\\
\Longrightarrow\quad & k = 0 \bmod q \qquad (\text{since } p - 1 \neq 0 \bmod q)\\
\Longrightarrow\quad & k \mid q\\
\Longrightarrow\quad & \alpha^k \in K.
\end{aligned}$$

This proves the lemma.

Now, using the fact that

$$x^q - x = \prod_{a \in L} (x - a)$$

we can write

$$\begin{aligned}
& x^q - x \mid f(x)^p - f(x)\\
\Longleftrightarrow\quad & \forall a \in L : x - a \mid f(x)^p - f(x)\\
\Longleftrightarrow\quad & \forall a \in L : f(x)^p - f(x) = 0 \bmod x - a\\
\Longleftrightarrow\quad & \forall a \in L : f(x)^p = f(x) \bmod x - a\\
\Longleftrightarrow\quad & \forall a \in L : f(a)^p = f(a)\\
\overset{\text{Lemma}}{\Longleftrightarrow}\quad & \forall a \in L : f(a) \in K
\end{aligned}$$

quod erat demonstrandum.

Ex. (24) $\boxed{\textbf{to be}}$

Ex. (25) Let $p_1 \cdot \dots \cdot p_r = u$ be a prime decomposition of u (note that $\mathbb{Z}[x]$ is factorial). In order to have u be not squarefree modulo some prime p we have to have $p_i = p_j \bmod p$ $(i \neq j)$. However, if $|p|$ is greater than two times the maximum coefficient of p_i and p_j, then it is ensured that "$p_i \bmod p = p_i \bmod \mathbb{Z}$," because the p_i are primitive since u is primitive by assumption. This means that $p_i \neq p_j$ in $\mathbb{Z}_p[x]$ because $p_i \neq p_j$ in $\mathbb{Z}[x]$. Now there are only finitely many p which satisfy the necessary condition which completes the proof.