Manuel Kauers
RISC-Linz

Hagenberg, December 17, 2002

Computer Algebra Exercises
Solution 3

Ex. (11) According to MAPLE, the polynomial $p(x) = x^3 + 2x + 1$ is irreducible over $\mathbb{Z}_3[x]$:[1]

```
>> Factor(x^3+2*x+1) mod 3;
```

$$x^3 + 2x + 1$$

```
>> p:=%:
```

So we can define $\mathrm{GF}(27) := \mathbb{Z}_3[x]/_{(p)}$. The following table shows all elements

$$b_2 x^2 + b_1 x + b_0 \in \mathrm{GF}(27)$$

as powers of x as well as their respective minimal polynomials.

n	x^n	b_2	b_1	b_0	min poly $/\mathbb{Z}_3$
$*$	0	0	0	0	x
0	1	0	0	1	$x+2$
1	x	0	1	0	$p(x)$
2	x^2	1	0	0	x^3+x^2+x+2
3	$x+2$	0	1	2	x^3+2x+1
4	x^2+2x	1	2	0	x^3+x^2+2
5	$2x^2+x+2$	2	1	2	x^3+2x^2+x+1
6	x^2+x+1	1	1	1	x^3+x^2+x+2
7	x^2+2x+2	1	2	2	x^3+x^2+2x+1
8	$2x^2+2$	2	0	2	x^3+2x^2+2x+2
9	$x+1$	0	1	1	x^3+2x+1
10	x^2+x	1	1	0	x^3+x^2+2
11	x^2+x+2	1	1	2	x^3+x^2+2x+1
12	x^2+2	1	0	2	x^3+x^2+2
13	2	0	0	2	$x+1$
14	$2x$	0	2	0	x^3+2x+2
15	$2x^2$	2	0	0	x^3+2x^2+x+1
16	$2x+1$	0	2	1	x^3+2x+2
17	$2x^2+x$	2	1	0	x^3+2x^2+1
18	x^2+2x+1	1	2	1	x^3+x^2+x+2
19	$2x^2+2x+1$	2	2	1	x^3+2x^2+x+1
20	$2x^2+x+1$	2	1	1	x^3+2x^2+2x+2
21	x^2+1	1	0	1	x^3+x^2+2x+1
22	$2x+2$	0	2	2	x^3+2x+2
23	$2x^2+2x$	2	2	0	x^3+2x^2+1
24	$2x^2+2x+1$	2	2	1	x^3+2x^2+2x+2
25	$2x^2+1$	2	0	1	x^3+2x^2+1
26	1	0	0	1	$x+2$

[1] By hand irreducibility can be checked via $p(0) = 1, p(1) = 1, p(2) = 1$.

According to p. 48 (and to Tobias ;-), the minimal polynomial for $\beta = x^k$ is given by the formula

$$m_\beta(y) = \prod_{i=0}^{2} (y - \beta^{3^i}).$$

In MAPLE,

```
>> m := k -> Rem((y-Rem(x^k, p, x) mod 3) *
>>      (y-Rem(x^(3*n), p, x) mod 3) *
>>      (y-Rem(x^(9*n), p, x) mod 3), p, x) mod 3;
```

defines a function m which maps $k \in \mathbb{N}_0$ to the minimal polynomial of $x^k \in \mathrm{GF}(27)$ over $\mathbb{Z}_3$.

Ex. (12) We need two irreducible polynomials $p_1, p_2 \in \mathbb{Z}_2[x]$ both of degree 3. Let's take

$$p_1(x) = x^3 + x + 1, \qquad p_2(x) = x^3 + x^2 + 1$$

and let $F_1 := \mathbb{Z}_2[x]/(p_1)$, $F_2 := \mathbb{Z}_2[x]/(p_2)$. We prove $F_1 \cong F_2$ by providing an isomorphism.

Using MAPLE, we verify that each of the two fields is generated by the polynomial $q(x) = x^2 + x + 1$. Let $i\colon F_1 \to F_2$ map $0 \in F_1$ to $0 \in F_2$ and each $a = q^{n_a} \bmod p_1 \in F_1$ to $q^{n_a} \bmod p_2 \in F_2$. Then i is an isomorphism: Take $a = q^{n_a} \bmod p_1, b = q^{n_b} \bmod p_1 \in F_1$. Then

$$\begin{aligned} i(a \cdot b) &= i(q^{n_a} \cdot q^{n_b} \bmod p_1) = i(q^{n_a + n_b} \bmod p_1) \\ &= q^{n_a + n + b} \bmod p_2 = q^{n_a} \cdot q^{n_b} \bmod p_2 \\ &= i(a) \cdot i(b), \\ i(a + b) &= i(q^{n_a} + q^{n_b} \bmod p_1) = q^{n_a} + q^{n_b} \bmod p_2 \\ &= i(a) + i(b). \end{aligned}$$

This completes the proof. ■.

Ex. (13) For the special case of constant $g = 0$ take $r = h = 0$. Now, assume $g \neq 0$. We furthermore assume $\deg f \geq 1$ to avoid trouble. Then $\deg f \leq \deg ff'$, so $\deg g < \deg ff'$. As f is square free, f and f' are relatively prime, so we can apply the corollary to Theorem 3.1.2., i.e. there are $u, v \in \mathbb{Q}[x]$ such that

$$g = uf + vf'$$

with $\deg u \leq \deg f' < \deg f$ and $\deg v < \deg f$ which can be computed by Euclid. We plug this into the integral, and start some calculation (using the fact that $n \geq 2$):

$$
\begin{aligned}
\int \frac{g(x)}{f(x)^n}\,dx &= \int \frac{u(x)f(x)+v(x)f'(x)}{f(x)^n}\,dx \\
&= \int \frac{u(x)}{f(x)^{n-1}}\,dx + \int \frac{f'(x)}{f(x)^n}\cdot v(x)\,dx \\
&= \int \frac{u(x)}{f(x)^{n-1}}\,dx - \frac{1}{n-1}\frac{v(x)}{f(x)^{n-1}} + \frac{1}{n-1}\int \frac{v'(x)}{f(x)^{n-1}}\,dx \\
&= \underbrace{-\frac{1}{n-1}\frac{v(x)}{f(x)^{n-1}}}_{=:r(x)} + \int \frac{\overbrace{u(x)-\frac{1}{n-1}v'(x)}^{=:h(x)}}{f(x)^{n-1}}\,dx.
\end{aligned}
$$

Note that indeed $\deg h < \deg f$ because $\deg v' \leq \deg v$ and both $\deg u$ and $\deg v$ are known to be less than $\deg f$ by construction. ■.

Ex. (14) Given two polynomials $u, v \in \mathbb{Z}_7[x]$:

$$
\begin{aligned}
u(x) &= 3x^6 + x^5 + 4x^4 + 4x^3 + 3x^2 + 4x + 1, \\
v(x) &= 2x^6 + 4x^5 + 3x^4 + 4x^3 + 4x^2 + x + 3.
\end{aligned}
$$

What is their gcd? Let's once again ask MAPLE for help.

```
>> Rem(u, v, x) mod 7;
```

$$2x^5 + 3x^4 + 5x^3 + 4x^2 + 6x + 1$$

```
>> Rem(v, %, x) mod 7;
```

$$x^3 + 3x^2 + 5x + 3$$

```
>> Rem(%%, %, x) mod 7;
```

$$x^2 + 2x + 2$$

```
>> Rem(%%, %, x) mod 7;
```

$$x + 1$$

```
>> Rem(%%, %, x) mod 7;
```

$$1$$

```
>> Rem(%%, %, x) mod 7;
```

$$0$$

So, $\gcd(u, v) = 1$.

Ex. (15) Without loss of generality, we may assume $m > n$. Because of $\mathrm{quot}(x^m - 1, x^n - 1) = x^{m-n}$ and

$$x^m - 1 - x^{m-n}(x^n - 1) = x^{m-n} - 1$$

we find as an invariant that u and v are always of the form $x^k - 1$ for some $k \in \mathbb{N}_0$, and that $\deg u$ keeps larger than $\deg v$.

We proceed to prove the claim that r, s, r', s' are always of the desired form by induction along the loop of the algorithm. For the induction start,

$$(u, r, s, v, r', s') = (x^m - 1, 1, 0, x^n - 1, 0, 1),$$

it is clear that r, s, r', s' are of the desired form.

As for the induction step, assume the state

$$(u, r, s, v, r', s') = (x^i - 1, r_0, s_0, x^j - 1, r'_0, s'_0)$$

where r_0, s_0, r'_0, s'_0 are of the desired form by IH. To get to the next step, we compute $q = \mathrm{quot}(u, v) = x^{i-j}$ and get

$$(u, r, s, v, r', s') \leftarrow (v, r'_0, s'_0, x^{i-j} - 1, r'_0 - x^{i-j} r_0, s'_0 - x^{i-j} s_0).$$

It turns out that the new r, s, r', s' are still of the desired form. ■.

For the special $u = x^{21} - 1, u = x^{13} - 1$, we find

$$\begin{aligned} x - 1 = \gcd(u, v) = & \underbrace{(x^{11} + x^8 + x^6 + x^3 + 1)}_{=r} \cdot u \\ & - \underbrace{(x^{19} + x^{16} + x^{14} + x^{11} + x^8 + x^6 + x^3 + x)}_{=s} \cdot v \end{aligned}$$