Oliver Tonnesen
V00885732

MATH 413

# Assignment 2

February 12, 2020

## 1

($\Rightarrow$): We prove the contrapositive. Let $f(x)$ be a quintic polynomial in $\mathbb{F}_p[x]$ with a zero in $\mathbb{F}_{p^2}$. If this zero is also in $\mathbb{F}_p$, then $f(x)$ is reducible in $\mathbb{F}_p[x]$, so suppose that $f(x)$ has no roots in $\mathbb{F}_p$. Then it has a root $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. We know that $\alpha$ is the root of an irreducible quadratic $g(x) \in \mathbb{F}_p[x]$, and that $\mathbb{F}_{p^2} \cong \mathbb{F}_p[x]/\langle g(x)\rangle$. This means that $g(x) \mid f(x)$, and so $f(x)$ is reducible in $\mathbb{F}_p[x]$. Thus we can conclude that if $f(x)$ is irreducible in $\mathbb{F}_p[x]$, then it has no roots in $\mathbb{F}_{p^2}$.

($\Leftarrow$): Again, we prove the contrapositive. Let $f(x)$ be a reducible quintic polynomial in $\mathbb{F}_p[x]$. If it has a root in $\mathbb{F}_p$, then it would also have a root in $\mathbb{F}_{p^2}$, so suppose it does not have any such roots. Then $f(x) = g(x)h(x)$ where WLOG $g(x)$ and $h(x)$ have degrees 3 and 2, respectively. This means $\mathbb{F}_p[x]/\langle h(x)\rangle \cong \mathbb{F}_{p^2}$, so $h(x)$ (and in turn $f(x)$) has a root in $\mathbb{F}_{p^2}$. Thus we can conclude that if $f(x)$ has no roots in $\mathbb{F}_{p^2}$, then it is irreducible in $\mathbb{F}_p[x]$.

## 2

### 2.a

$f(x) = x^6 + 2x^4 + x + 2$, and $f'(x) = 2x^3 + 1$. The gcd calculation is fairly straightforward, and in fact $f'(x) \mid f(x)$. In characteristic 3, $f'(x) = 2x^3 + 1 = (2x)^3 + 1^3 = (2x+1)^3$, so $(2x+1)^3 \mid f(x)$, and $f(x)$ is thus not separable.

### 2.b

As we saw, $f'(x) \mid f(x)$, and $\frac{f(x)}{f'(x)} = 2x^3 + x + 2 = x^3 + 2 + 1$. Thus $f(x) = f'(x)(x^3 + 2x + 1) = (2x+1)^3(x^3 + 2x + 1)$, and so we need only find a field in which $x^3 + 2x + 1$ splits.

It is straightforward to check that $x^3 + 2x + 1$ has no roots in $\mathbb{F}_9$, so we skip straight to $\mathbb{F}_{27}$.

Note that $x^3 + 2x + 1$ has no roots in $\mathbb{F}_3$, so since its degree is 3, it is irreducible, and so $\mathbb{F}_3[x]/\langle x^3 + 2x + 1\rangle$ is a field of order $3^3$. Let $\alpha^3 + 2\alpha + 1 = 0$, and consider $\mathbb{F}_3(\alpha)$:

In $\mathbb{F}_3(\alpha)[x]$, $x^3 + 2x + 1$ has a root at $x = \alpha$, so $x - a \mid x^3 + 2x + 1$, and $\frac{x^3+2x+1}{x-a} = x^2 + \alpha x + 2 + \alpha^2$. We see that $x^2 + \alpha x + 2 + \alpha^2$ further factors over $\mathbb{F}_3(\alpha)$ into $(x+2\alpha+2)(x+2\alpha+1)$, so in the end, we have that in $\mathbb{F}_3(\alpha)[x]$, $f(x) = (2x+1)^3(x+2\alpha)(x+2\alpha+2)(x+2\alpha+1)$, so $f$ splits in $\mathbb{F}_3(\alpha)$.

# 3

Note that $g(x) = \frac{x^p-1}{x-1}$. We know that the number of irreducible factors of $x^n - 1$ in $\mathbb{F}_2[x]$ is the number of orbits of the doubling map in $\mathbb{Z}/n\mathbb{Z}$.

($\Rightarrow$): We prove the contrapositive. Suppose 2 is not a primitive root mod $p$. Then its orbit in the doubling map has size less than $p-1$. The orbit of 0 always has size 1, and so there must be a third orbit. This means that $x^p - 1$ has at least three irreducible factors. We know that $x-1$ is irreducible, and that $x^p - 1 = g(x)(x-1)$, so it must be the case that $g(x)$ is reducible. Thus we can conclude that if 2 is a primitive root mod $p$ that $g(x)$ is irreducible.

($\Leftarrow$): 2 is a primitive root mod $p$, so its orbit has size $p-1$, with 0 generating the $\{0\}$ orbit. Thus $x^p - 1$ has two irreducible factors. $x^p - 1 = g(x)(x-1)$, and $x-1$ is irreducible, so $g(x)$ is irreducible.

This proof should work as long as 2 is a primitive root mod $n$, since the proof relies on 2's orbit in the doubling map being full, and has nothing to do with $n$'s primality.

# 4

## 4.a

The $N$th cyclotomic polynomial is $\Phi_N(x) = (x-\zeta_1)\cdots(x-\zeta_{\varphi(N)})$. Evaluated at 0, this is simply the product of the primitive roots of unity: $\Phi_N(0) = (-\zeta_1)\cdots(-\zeta_{\varphi(N)})$. If $\zeta_k$ is a primitive root of unity, then so is $\frac{1}{\zeta_k}$, so since $\varphi(N)$ is even whenever $N > 3$, we can simply pair off the primitive roots of unity in our product to get $\Phi_N(0) = (-\zeta_1)(\frac{1}{-\zeta_1})\cdots(-\zeta_{\varphi(N)})(\frac{1}{-\zeta_{\varphi(N)}}) = 1$. Otherwise we see $\Phi_2(0) = (0)+1$ and $\Phi_3(0) = (0)^2+(0)+1$, and so $\Phi_N(0) = 1$ for any $N \geq 2$.

### 4.b

We know that $x^N - 1 = \prod_{d|N} \Phi_d(x)$, so

$$\begin{aligned} x^{pq} - 1 &= \prod_{d|pq} \Phi_d(x) \\ &= \Phi_{pq}(x)\Phi_p(x)\Phi_q(x)\Phi_1(x) \\ &= \Phi_{pq}(x)\Phi_p(x)\Phi_q(x)(x-1). \end{aligned}$$

Dividing by $x - 1$, we get

$$x^{pq-1} + \cdots + 1 = \Phi_{pq}(x)\Phi_p(x)\Phi_q(x).$$

We also know that for $p$ a prime, $\Phi_p(x) = 1 + \cdots + x^{p-1}$, so we get

$$\Phi_{pq}(x) = \frac{x^{pq-1} + \cdots + 1}{(1 + \cdots + x^{p-1})(1 + \cdots + x^{q-1})}.$$

Finally, plugging in $x = 1$, we get $\Phi_{pq}(1) = \frac{1^{pq-1}+\cdots+1}{(1+\cdots+1^{p-1})(1+\cdots+1^{q-1})} \frac{pq}{(p)(q)} = 1$, as desired.

## 5

The generating function has the form $G(x) = \frac{1}{1-2x+x^3}$, so the characteristic polynomial of its coefficient sequence is $x^3 - 2x + 1$. This means the sequence is $s_{n+3} = 2s_{n+2} - s_n$. Now we simply need to find the initial conditions $s_0$, $s_1$, and $s_2$. Rewriting $G(x)$ as a formal power series, we get $\sum_{n=0}^{\infty} s_n x^n = \frac{1}{1-2x+x^3}$, and rearranging, we get $(\sum_{n=0}^{\infty} s_n x^n)(1 - 2x + x^3) = 1$. Now we can simply match coefficients to obtain

$$\begin{aligned} s_0 x^0 &= 1 \\ -2s_0 x + s_1 x &= 0 \\ -2s_1 x^2 + s_2 x^2 &= 0 \end{aligned}$$

Plugging $x = -1$ into the last two equations, we get $s_1 = 2$ and $s_2 = 4$. In the end, we end up with the recurrence $s_{n+3} = 2s_{n+2} - s_n$ with initial conditions $s_0 = 1$, $s_1 = 2$, and $s_2 = 4$.

# 6

## 6.a

$\mathbb{F}_p^\times$ is cyclic of order $p-1$, so for any $x \in \mathbb{F}_p^\times$, $x^{p-1} = 1$. If $x$ is square – that is, $x = y^2$ for some $y$ – then since $y^{p-1} = 1$, $(y^2)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}} = 1$. If $x^{\frac{p-1}{2}} \neq 1$, then $(x^{\frac{1}{2}})^{p-1} \neq 1$, so $x^{\frac{1}{2}} \notin \mathbb{F}_p^\times$, so $x$ is not square. So if $x$ is not square, then $x^{\frac{p-1}{2}} \neq 1$, but we know that $x^{p-1} = 1$, so $x^{\frac{p-1}{2}}$ must be $-1$. Thus we take $f(x)$ to be $x^{\frac{p-1}{2}}$, and the condition is satisfied.

## 6.b

We construct the Vandermonde matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 & 1 \\ 1 & 3 & 4 & 2 & 1 \\ 1 & 4 & 1 & 4 & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 1 \\ 2 \\ 0 \end{pmatrix}$$

After row reduction, we get:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 3 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 4 \\ 4 \\ 4 \end{pmatrix}$$

Finally, substituting back in, we get $c_4 = 4$, $c_3 = 0$, $c_2 = 4$, $c_1 = 1$, and $c_0 = 1$, giving us $f(x) = 4x^4 + x^2 + x + 1$.

# 7

## 7.a

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix}$$

## 7.b

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$