Oliver Tonnesen
V00885732

Assignment 1

MATH 413
January 24, 2020

1

We see that $n + 16 = 62773929 = 7923^2$ is a square integer. This gives us $n + 4^2 = 7923^2$, so

$$\begin{aligned} n &= 7923^2 - 4^2 \\ &= (7923 + 4)(7923 - 4) \\ &= 7919 \cdot 7927 \end{aligned}$$

This insecurity might be avoided by ensuring p and q do not differ by a square. If they do, then it is straightforward to try the above technique with all numbers around $\sqrt{n}$, eventually finding the correct factorization.

2

2.a

It's clear to see that $\gcd(22, 5) = 1$, so 5 is a primitive 22nd root of unity, and thus generates $\mathbb{F}_{23}^{\times}$.

$|\langle 5 \rangle| = 22$, so we know $5^{22} = 1$. Thus $(5^2)^{11} = 1$, so $\left|\langle 5^2 \rangle\right| = |\langle 2 \rangle| \leq 11$, so 2 is not a generator of $\mathbb{F}_{23}^{\times}$.

2.b

We know the polynomial $x^{23} - x$ in $\mathbb{F}_{23}[x]$ contains all the elements of $\mathbb{F}_{23}$ as roots, so if $x^2 + x + 1 = 0$ has a root in $\mathbb{F}_{23}$, then $\gcd(x^{23} - x, x^2 + x + 1) \neq 1$. Some straightforward calculations give us $\gcd(x^{23} - x, x^2 + x + 1) = 18$. The gcd in a field is only defined up to multiplication by a constant, so this means 1 is also a gcd. Thus it must be the case that $x^2 + x + 1$ has no roots in $\mathbb{F}_{23}$.

3

3.a

If $q = 2$, then $\sum_{a \in \mathbb{F}_q^+} = 1$. If $q = 2^k$, $k > 1$, then $\mathbb{F}_q^+ \cong \bigoplus_{i=1}^{k} \mathbb{Z}_2$.

Thus if we label the elements of $\mathbb{F}_q^+$ as $(r_1, \ldots, r_k)$, then for any r_i, there are exactly 2^{k-1} elements in which it is 0, and 2^{k-1} in which it is 1. So adding together all elements leaves us with $(0, \ldots, 0)$, since each spot in the tuple is the sum of an even number of 1s (and an even number of 0s).

Otherwise, if $q = p^k$, $p \neq 2$ a prime, $k \geq 1$, then $\mathbb{F}_q^+ \cong \bigoplus_{i+1}^k \mathbb{Z}_p$. Then the sum in each slot is

$$\begin{aligned} 1 + \cdots + p - 1 &= (1 + p - 1) + (2 + p - 2) + \cdots + \left(\left\lfloor \frac{p}{2} \right\rfloor + \left\lceil \frac{p}{2} \right\rceil \right) \\ &= 0 + 0 + \cdots + 0 \\ &= 0 \end{aligned}$$

since p is odd, and so we end up with $(0, \ldots, 0)$.

3.b

We know that $\mathbb{F}_q^\times$ is cyclic is order $q-1$, so let $\langle g \rangle = \mathbb{F}_q^\times$. Then $\prod_{a \in \mathbb{F}_q^\times} = g^1 \cdot g^2 \cdot \ldots \cdot g^{q-1} = g^{\frac{(q-1)(q-1+1)}{2}} = g^{\frac{q^2-q}{2}}$. If $q \neq 2$, then $q-1$ is even. This means $\frac{q^2-q}{2} = q\frac{q-1}{2} = qk$ for $k = \frac{q-1}{2}$. Notice that k is an integer. So $g^1 \cdot g^2 \cdot \ldots \cdot g^{q-1} = g^{qk} = (g^q)^k = g^k$. Thus

$$\prod_{a \in \mathbb{F}_q^\times} = g^k = g^{\frac{q-1}{2}} = g^{\frac{|\mathbb{F}_q|}{2}} = -1 = q - 1.$$

4

4.a

Suppose not. Then there are some non-units $g(x), h(x) \in \mathbb{F}_2[x]$, with $g(x)h(x) = x^5 + x^3 + 1$. $x^5 + x^3 + 1$ clearly has no degree one factors, so WLOG $g(x)$ and $h(x)$ must have degree two and three, respectively. That is, $g(x) = ax^2 + bx + c$, and $h(x) = qx^3 + rx^2 + sx + t$. Then

$$g(x)h(x) = aqx^5 + (ar+bq)x^4 + (as+br+cq)x^3 + (at+bs+cr)x^2 + (bt+cs)x + ct.$$

So we have:

$$\begin{aligned} aq &= 1 && (1) \\ ar + bq &= 0 && (2) \\ as + br + cq &= 1 && (3) \\ at + bs + cr &= 0 && (4) \\ bt + cs &= 0 && (5) \\ ct &= 1 && (6) \end{aligned}$$

By (1), $a = q = 1$. Then (2) gives $ar + bq = r + b = 0$, so $b = r$. (3) gives us $as + br + cq = s + br + c = 0$. By (6), $t = 1$, so (4) gives us $at + bs + cr = at + bs + cb = at + b(s + c) = 0$. $a = t = 1$, so $at = 1$. Thus $b(s + c) = 1$. Then $s + c = 1$. $b = r$, so $r = 1$, but this means $s + br + c = br + (s + c) = 0$, a contradiction, since by (3), $as + br + cq = s + br + c = 1$. So no such $g(x), h(x)$ exist, and thus $x^5 + x^3 + 1$ is irreducible in $\mathbb{F}_2[x]$.

4.b

No. It would always have a root at $x = 1$, and would thus factor into the monomial (x+1) and some other polynomial.

5

5.a

Let $\alpha^2 + \alpha + 7 = 0$. Then $\langle\alpha\rangle = \mathbb{F}_{121}^\times$. So $|\alpha| = 120$. Consider α^k. $\langle\alpha\rangle = \{1, \alpha^k, \ldots, \alpha^{\frac{120}{\gcd(120,k)}}\}$, so $\left|\alpha^k\right| = 120$ when $\gcd(120, k) = 1$. Thus our generators are all a^k with $\gcd(120, k) = 1$, so $\mathbb{F}_{121}$ has $\varphi(120)$ generators.

5.b

α^{30}

5.c

α^{24}

6

In order for $\mathbb{F}_{p^m}$ to be a subfield of $\mathbb{F}_{p^n}$, it must be the case that $m \mid n$. So the subfields of $\mathbb{F}_{p^{p^2}}$ are all the $\mathbb{F}_{p^m}$ such that $m \mid p^2$. Thus $m = 1, p$. So all the subfields of $\mathbb{F}_{p^{p^2}}$ are $\mathbb{F}_p$ and $\mathbb{F}_{p^p}$. The containment is as follows: $\mathbb{F}_p \subsetneq \mathbb{F}_{p^p} \subsetneq \mathbb{F}_{p^{p^2}}$

7

7.a

Let $l \in \mathbb{L}$. We know that $\{a_1, \ldots, a_m\}$ is a basis of $\mathbb{L}$ over $\mathbb{K}$, so

$$l = a_1 k_1 + \ldots + a_m k_m$$

where $k_i \in \mathbb{K}$. Similarly, $\{b_1, \ldots, b_n\}$ is a basis of $\mathbb{K}$ over $\mathbb{F}$, so for each k_i,

$$k_i = b_1 f_{i1} + \ldots + b_n f_{in}$$

where $f_{ij} \in \mathbb{F}$. This means our arbitrarily chosen l can be rewritten as

$$\begin{aligned} l &= a_1(b_1 f_{11} + \ldots + b_n f_{1n}) + \ldots + a_m(b_1 f_{m1} + \ldots + b_n f_{mn}) \\ &= a_1 b_1 f_{11} + a_1 b_2 f_{12} + \ldots + a_m b_n f_{mn} \in \mathrm{Span}\{a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}, \end{aligned}$$

so the above is indeed a basis of $\mathbb{L}$ over $\mathbb{F}$, as desired.

7.b

$\{1, \sqrt[3]{2}, i\}$