

Frank Moore
Math 918, Taught by Jon-Lark Kim
Homework 2
Week of July 28th

Problem 1: Suppose l is prime, and $f = l^n$. Find a simple formula for the number of monic irreducible polynomials of degree f over \mathbb{F}_p .

Note that the formula in the book suggests that the answer is $n_f = (p^f - \sum_d dn_d)/f$, where the sum is taken over all $d < f$ that divide f . We wish to obtain a simpler formula. First, I claim that $\sum_d dn_d = p^{f/l}$. We proceed by induction on n . Note for the case $n = 0$, we have that there are p irreducible linear polynomials, one for each element of \mathbb{F}_p . To use the induction, we immediately have:

$$\begin{aligned} \sum_d dn_d &= \left(\sum_{i=1}^{n-1} l^i n_i \right) + n_1 \\ &= \left(\sum_{i=1}^{n-1} l^i (p^{l^i} - p^{l^{i-1}})/l^i \right) + p \quad (\text{induction}) \\ &= \left(\sum_{i=1}^{n-1} (p^{l^i} - p^{l^{i-1}}) \right) + p \\ &= -p + p^{l^{n-1}} + p \quad (\text{telescoping sum}) \\ &= p^{f/l} \end{aligned}$$

As desired. Therefore, substituting in for $\sum_d dn_d$ above, we have $n_f = (p^f - p^{f/l})/f$.

Problem 2: Suppose $\alpha \in \mathbb{F}_{p^2}$ satisfies $x^2 + ax + b = 0$ where $a, b \in \mathbb{F}_p$.

Part a: Show that α^p is also a root of the above polynomial.

Note that since \mathbb{F}_{p^2} is a field of characteristic p , we have that

$$\begin{aligned} (\alpha^p)^2 + a\alpha^p + b &= (\alpha^p)^2 + a^p\alpha^p + b^p \quad (\text{as } a, b \in \mathbb{F}_p) \\ &= (\alpha^p)^2 + (a\alpha)^p + b^p = (\alpha^2 + a\alpha + b)^p = 0^p = 0 \end{aligned}$$

Therefore, α^p is a root of the above polynomial.

Part b: Suppose that $\alpha \notin \mathbb{F}_p$. Show that $a = -\alpha - \alpha^p$ and $b = \alpha^{p+1}$.

So, if $\alpha \notin \mathbb{F}_p$, then we have $\alpha^p \neq \alpha$. Therefore, α and α^p are the two distinct roots of the above quadratic equation. Therefore by common algebra, a is the negative of their sum and b is their product. Hence, $a = -(\alpha + \alpha^p)$ and $b = \alpha^{p+1}$.

Part c: Suppose that $\alpha \notin \mathbb{F}_p$, and $c, d \in \mathbb{F}_p$. Show that $(c + \alpha d)^{p+1} = d^2 - acd + bc^2 \in \mathbb{F}_p$.

Note that $(c + \alpha d)^{p+1} = (c + \alpha d)^p(c + \alpha d) = (c^p + \alpha^p d^p)(c + \alpha d) = (c + \alpha^p d)(c + \alpha d)$. Therefore, multiplying this out, we have that $(c + \alpha d)^{p+1} = c^2\alpha^{p+1} + cd\alpha^p + cd\alpha + d^2 = d^2 - acd + bc^2$.

Part d: Suppose $i = \sqrt{-1} \in \mathbb{F}_{19^2}$. Use (c) to find $(2 + 3i)^{101}$ in the form $a + bi$ for some $a, b \in \mathbb{F}_{19}$.

Using the setup as above, we have $x^2 + 1 = 0$, or in the above lemma, $b = 0$ and $c = 1$. Therefore, we have

$(2+3i)^{20} = 13$. Now $(2+3i)^{101} = ((2+3i)^{20})^5(2+3i) = (13^5)(2+3i) = 14(2+3i) = (-5(2+3i)) = (9+4i)$.

Problem 3: Find $\left(\frac{1801}{8191}\right)$ using two methods. One using Legendre symbols only to reduce the symbol (requires factoring) and the other using Jacobi symbols (requires only factoring out powers of 2).

The method of calculating Legendre symbols is just following their basic rules. This is the method that requires factoring:

$$\begin{aligned} \left(\frac{1801}{8191}\right) &= \left(\frac{8191}{1801}\right) = \left(\frac{987}{1801}\right) = \left(\frac{3}{1801}\right) \left(\frac{7}{1801}\right) \left(\frac{47}{1801}\right) \\ &= \left(\frac{1801}{3}\right) \left(\frac{1801}{7}\right) \left(\frac{1801}{47}\right) = \left(\frac{1}{3}\right) \left(\frac{2}{7}\right) \left(\frac{15}{47}\right) \\ &= 1 \cdot (-1)^6 \cdot \left(\frac{3}{47}\right) \left(\frac{5}{47}\right) = - \left(\frac{47}{3}\right) \left(\frac{47}{5}\right) = - \left(\frac{2}{3}\right) \left(\frac{2}{5}\right) = -(-1)^1(-1)^3 = -1 \end{aligned}$$

Using the generalized Jacobi symbols (with similar rules as the Legendre symbol) requires only factoring powers of 2 from the top number:

$$\begin{aligned} \left(\frac{1801}{8191}\right) &= \left(\frac{8191}{1801}\right) = \left(\frac{987}{1801}\right) = \left(\frac{1801}{987}\right) = \left(\frac{814}{987}\right) = \left(\frac{2}{987}\right) \left(\frac{407}{987}\right) \\ &= -(-1) \left(\frac{987}{407}\right) = \left(\frac{173}{407}\right) = \left(\frac{407}{173}\right) = \left(\frac{61}{173}\right) = \left(\frac{173}{61}\right) = \left(\frac{51}{61}\right) \\ &= \left(\frac{61}{51}\right) = \left(\frac{10}{51}\right) = \left(\frac{2}{51}\right) \left(\frac{5}{51}\right) = (-1) \left(\frac{1}{51}\right) = -1 \end{aligned}$$

Problem 4: Let $p = 2081$ and n the smallest positive nonresidue mod p . Find n and use the method in the test to find the square root of 302 mod p .

Note that as $(-1)^{(2081^2-1)/8} = 1$, we know that 2 is a residue mod 2081. However, $\left(\frac{3}{2081}\right) = \left(\frac{2081}{3}\right) = \left(\frac{2}{3}\right) = (-1)$. Therefore, $n = 3$ is the smallest nonresidue mod p . Now to set up the variables, $p-1 = 2^5 \cdot 65$, so $\alpha = 5$, and $s = 65$. $b = n^s = 3^{65} = 888 \pmod{p}$. $r = a^{(s+1)/2} = a^{33} = 203 \pmod{p}$. Also, note that $a^{-1} = 820$ and may be found with a CAS or the Euclidean Algorithm. Now $(a^{-1}r^2)^{2^3} = 1 \pmod{p}$, so that $j_0 = 0$. Also, $(a^{-1}r^2)^{2^2} = 1 \pmod{p}$, so that $j_1 = 0$. Furthermore, $(a^{-1}r^2)^{2^1} = -1 \pmod{p}$ so we choose $j_2 = 1$. Now, we try $(a^{-1}(b^4r)^2) = 1$, so that $j_3 = 0$. Therefore, we have b^4r is the square root of 302 mod p . Calculating this, we have $b^4r = 1292$ (thanks to Maple for the modular arithmetic).

Problem 5: Decode the message "OFJDFOHFXOL" assuming that you know the message is being encoded with an affine cypher using single letter message blocks. Also assume that you know the message begins with "I". The alphabet being used is the 27 letter alphabet - space is 26.

So, setting up our equations, we have:

$$5 \equiv b - a \pmod{27}$$

$$14 \equiv 8a + b \pmod{27}$$

Solving this equation for a gives $9 \equiv 9a \pmod{27}$. So, we have a problem, as 9 does not have a multiplicative inverse mod 27 because $\gcd(9, 27) = 9$. We know that $b = 5 + a$, and that a can be 1,4,7,10,13,16,19,22,25. So, we begin to check these 9 possibilities. Checking $a = 1$ does not lead to a meaningful word for the second word (since we know the second word is two letters long by converting all "F" to " "). Indeed, with this choice we end up with the first word being "DX". Checking $a = 4$ we get a meaningful word for the second word, "AM". Trying the rest of the message gives one that makes sense, "I AM IN RIO".