

Frank Moore
Math 918, Taught by Jon-Lark Kim
Homework 3
Due August 12th

Problem 1: Using Ex. 16-18, section III.2, find a formula for the number of elements in the set $M_2(\mathbb{Z}/N\mathbb{Z})^*$ of invertible matrices mod N . Write your formula in a similar form for the number $\phi(N) = N \prod_{p|N} (1 - \frac{1}{p})$ of invertible elements in $\mathbb{Z}/N\mathbb{Z}$. How many possible 2×2 enciphering matrices A are there when $N = 26, 29, 30$?

The results from problem 16 and 18 give $|M_2(\mathbb{Z}/p^\alpha\mathbb{Z})^*| = p^{4\alpha-3}(p^2-1)(p-1)$, and $|M_2(\mathbb{Z}/N\mathbb{Z})^*| = |M_2(\mathbb{Z}/n\mathbb{Z})^*| \cdot |M_2(\mathbb{Z}/m\mathbb{Z})^*|$ where $N = mn$ and $\gcd(m, n) = 1$. So, say $N = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. Then we immediately have:

$$\begin{aligned} |M_2(\mathbb{Z}/N\mathbb{Z})^*| &= \prod_{i=1}^n |M_2(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*| \\ &= \prod_{i=1}^n p_i^{4\alpha_i-3}(p_i^2-1)(p_i-1) \\ &= \prod_{p|n} p^4 \left(1 - \frac{1}{p^2}\right) \left(1 - \frac{1}{p}\right) \\ &= N^4 \prod_{p|n} \left(1 - \frac{1}{p^2}\right) \left(1 - \frac{1}{p}\right), \text{ as desired} \end{aligned}$$

Now, plugging in $N = 26, 29, 30$ we get $|M_2(\mathbb{Z}/N\mathbb{Z})^*| = 157248, 682080, 138240$ respectively.

Problem 2: We are trying to send the message "SEND \$7500" to a user using the RSA cryptosystem that has the public key (2047,179). The alphabet we are using is 0-25 are the letters, space=26, .=27, ?=28, \$=29, 30-39 are the numbers 0-9. Also, we are to embed the message using digraphs and transmit the encrypted message using trigraphs. Therefore, converting the message to numbers, we have the sequence {724, 523, 1069, 1515, 1230}. Raising each message unit to 179, we get the message units, {1906, 1072, 802, 364, 710}. Converting this to letters, we got the message {(BH), (A 2), (AUC), (AJE), (AR0)}. Note that $2047 = 23 \cdot 89$. Therefore we get $\phi(2047) = 2047 - 23 - 89 + 1 = 1936$. Computing the inverse of 179 mod 2047, we obtain 411. This allows us to decrypt the message back to "SEND \$7500".

Problem 3: Using the Silber-Pohlig Hellman algorithm, find the discrete log of 153 to the base 2 in \mathbb{F}_{181}^* .

Notice that $q - 1 = 181 - 1 = 2^2 \cdot 3^2 \cdot 5$. Now, for 2,3, and 5, we create a list of numbers $r_{p,j}$ which are the various p th roots of unity for $p = 2, 3, 5$. To do this, we calculate $r_{p,j} = b^{j(q-1)/p}$, for each $p | q - 1$ and $j = 0, \dots, p - 1$. Our list is as follows:

$$\begin{array}{lll} r_{2,0} = 1 & r_{3,0} = 1 & r_{5,0} = 1 \\ r_{2,1} = -1 & r_{3,1} = 48 & r_{5,1} = 59 \\ & r_{3,2} = 132 & r_{5,2} = 42 \\ & & r_{5,3} = 125 \\ & & r_{5,4} = 135 \end{array}$$

We will work through the next step in detail for $p = 2$ and leave the details of the rest out, as they are identical in nature. So, we are trying to find $x \pmod{q - 1}$ such that $2^x \equiv 153 \pmod{181}$. So, it suffices to find the moduli for each prime power dividing 180. So, write $x \equiv x_0 + 2x_1 \pmod{4}$. Then following the method in the text, we compute 153^{90} and get -1 . Therefore, we compare this to the table of $r_{2,j}$ and find that $x_0 = 1$. Setting $y' = y/b^{x_0}$, we get $y' = 167$. Computing $167^{45} \pmod{181}$, we obtain -1 again. Therefore, we see that $x_1 = 1$. Hence, $x \equiv 3 \pmod{4}$. Doing this same calculation for 3 and 5, we see that $x \equiv 8 \pmod{9}$ and $x \equiv 2 \pmod{5}$. Therefore, using the Chinese Remainder Theorem to obtain the solution to the above system of equivalences, we get that $x = 107$. Checking our answer, we see that $2^{107} \equiv 153 \pmod{181}$.