

DISCRETE MATHEMATICS
HOMEWORK 4

1. We have conjectured in class that $1/k$ does not exist in \mathbb{Z}_m if $\gcd(k, m) > 1$. As far as we can tell so far, $1/k$ *does* exist in \mathbb{Z}_m if $\gcd(k, m) = 1$. Try to explore these conjectures, giving persuasive arguments (proofs?) for as much of this as you can.
2. Here are a couple on Diophantine equations:
 - (a) Find solutions in the integers to the equation $29x - 62y = 1$. Convince me that any solutions you find actually work. Ideally, convince me you have found all the solutions.
 - (b) Do the same thing with the equation $35x - 154y = 1$.
 - (c) Explain again what these problems have to do with the problems of finding $1/29$ in \mathbb{Z}_{62} and $1/35$ in \mathbb{Z}_{154} . Find these fractions if they exist.
3. Compute the following gcds:
 - (a) $\gcd(385313, 337976)$.
 - (b) $\gcd(2288702, 762185)$.
4. Convince me of the truth or falsehood of the following claims:
 - (a) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
 - (b) If $a \mid b$ and $a \mid c$, then $a \mid (bx - c)$.
5. The attached table comes from Carl Friedrich Gauss' *Disquisitiones Arithmeticae*, one of the most important works in the history of number theory, published in 1801 when Gauss was 24. Gauss was interested in the question of when \sqrt{p} exists in \mathbb{Z}_q . His investigations and those of his predecessors had led him to where he could answer this question as long as he could answer it when q was an odd prime and when p was either -1 or a prime. Gauss therefore made a table of when \sqrt{p} exists in \mathbb{Z}_q when p and q satisfy these constraints and are less than 100. This is the attached Table 2. The little bars indicate square roots that **do** exist; so for example, the first column of the table tells you that $\sqrt{-1}$ exists in $\mathbb{Z}_5, \mathbb{Z}_{13}, \mathbb{Z}_{17}, \mathbb{Z}_{29}$ and so on, and that it does not exist in $\mathbb{Z}_3, \mathbb{Z}_7, \mathbb{Z}_{11}, \mathbb{Z}_{19}, \mathbb{Z}_{23}$ and so on. The second column shows the q for which $\sqrt{2}$ exists in \mathbb{Z}_q , etc. Look at Gauss' table, and see if you notice anything at all. Any observation you can make will be interesting. Some possibly useful hints:
 - (1) It was already known before Gauss' time that numbers which were 1 more than a multiple of 4 and numbers which were 1 less than a multiple of 4 were different.
 - (2) The final theorem Gauss proved to answer this question is called *Quadratic Reciprocity*.
 - (3) I'm not suggesting that you look up quadratic reciprocity.
 - (4) There is exactly one typo in Gauss' table, which was pointed out to me in this class in 2003 by Holley Lynch.

