University of Waterloo
Faculty of Mathematics

Centre for Education in
Mathematics and Computing

Senior Math Circles
October 22, 2008
Number Theory III

Number Theory

Perfect Squares

	mod 3	mod 4	mod 5	mod 6	mod 7	mod 8	mod 9	mod 11
1	1	1	1	1	1	1	1	1
4	1	0	4	4	4	4	4	4
9	0	1	4	3	2	1	0	9
16	1	0	1	4	2	0	7	5
25	1	1	0	1	4	1	7	3
36	0	0	1	0	1	4	0	3
49	1	1	4	1	0	1	4	5
64	1	0	4	4	1	0	1	9
81	0	1	1	3	4	1	0	4
100	1	0	0	4	2	4	1	1

Definition:
For positive integers a and n with $0 < a < n$, if $x^2 \equiv a \mod n$ has a solution, then we say a is a *quadratic residue* $\mod n$.

For example, the quadratic residues of 11 are 1, 3, 4, 5, and 9.

Legendre Symbol

If $\gcd(a, p) = 1$, then we can define the following function.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue } \mod p \\ -1 & \text{if } a \text{ is not a quadratic residue } \mod p \end{cases}$$

Examples:
$\left(\frac{2}{11}\right) = -1$
$\left(\frac{4}{8}\right) = 1$

Theorem (Euler's Criterion):
If p is an odd prime and $\gcd(a,p)=1$, then $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \mod p$.

Example:

$$\begin{aligned}(\tfrac{2}{127}) &\equiv 2^{\frac{127-1}{2}} \mod 127\\ &\equiv 2^{63} \mod 127\end{aligned}$$

We know $2^7 \equiv 128 \equiv 1 \mod 127$, so $2^{63} \equiv (2^7)^9 \equiv 1 \mod 127$.
Therefore 2 is a quadratic residue $\mod 127$.

$$\begin{aligned}(\tfrac{5}{127}) &\equiv 5^{\frac{127-1}{2}} \mod 127\\ &\equiv 5^{63} \mod 127\\ &\equiv (5^3)^{21} \mod 127\\ &\equiv (-2)^{21} \mod 127\\ &\equiv (-128)^7 \mod 127\\ &\equiv (-1)^7 \mod 127\\ &\equiv -1 \mod 127\end{aligned}$$

Therefore, 5 is not a quadratic residue $\mod 127$.

Quadratic Congruences

To find solutions to the quadratic congruence $ax^2+bx+c \equiv 0 \mod p$, where p is a prime, we do the following.

$$\begin{aligned}ax^2+bx+c &\equiv 0 \mod p\\ 4a^2x^2+4abx+4ac &\equiv 0 \mod p\\ 4a^2x^2+4abx+b^2-b^2+4ac &\equiv 0 \mod p\\ (2ax+b)^2 &\equiv b^2-4ac \mod p\end{aligned}$$

Now, we let $y=2ax+b$ so the congruence becomes $y^2 \equiv b^2-4ac \mod p$.

Example: Solve $5x^2+4x+7 \equiv 0 \mod 19$.

$$\begin{aligned}y^2 &\equiv 16-4(5)(7) \mod 19\\ y^2 &\equiv 9 \mod 19\end{aligned}$$

So $y \equiv 3 \mod 19$ or $y \equiv -3 \equiv 16 \mod 19$.

Thus
$$\begin{aligned}10x+4 &\equiv 3 \mod 19\\ 10x &\equiv -1 \mod 19\\ x &\equiv -2 \mod 19\\ x &\equiv 17 \mod 19\end{aligned}$$
or
$$\begin{aligned}10x+4 &\equiv 16 \mod 19\\ 10x &\equiv 12 \mod 19\\ x &\equiv 24 \mod 19\\ x &\equiv 5 \mod 19\end{aligned}$$

Problem:
Solve $3x^2+15x+9 \equiv 0 \mod 17$.

Magic Squares

An $n \times n$ magic square is a grid with n rows and n columns, that is filled in with numbers so that the sum of each row, each column, and each main diagonal is the same. This sum is called the magic constant.

Problem: Solve the following magic square.

16			13
5		11	
		7	12
4			

Uniform Step Method

To create an n by n magic square containing the numbers $0, 1, \ldots, n^2 - 1$ and having a magic constant of $\frac{n(n^2-1)}{2}$, we can use this method.
Let a, b, c, d, e, and f be positive integers such that $\gcd(cf - de, n) = 1$.
Label the rows and the columns of the magic square with the numbers $1, 2, \ldots, n-1, n$.
Then, put each of the numbers $j = 0, 1, \ldots, n^2 - 1$ into the cell with coordinates:
$x_j \equiv a + cj + e\lfloor \frac{j}{n} \rfloor \mod n$
$y_j \equiv b + dj + f\lfloor \frac{j}{n} \rfloor \mod n$
Note that $\lfloor x \rfloor$ is the largest integer that is less than or equal to x. For example, $\lfloor 0 \rfloor = 0$ and $\lfloor \frac{8}{3} \rfloor = 2$.

Example: Fill in the following magic square.

	1			
0				

Let's label the columns from left to right as 1,2,3,4,5, and the rows from top to bottom as 5,4,3,2,1.
For $j = 0$, $x_0 = 1$ and $y_0 = 1$, therefore $a = 1$ and $b = 1$.

Also, since $x_1 = 2$ and $y_1 = 3$, therefore $2 \equiv 1 + c(1) + e\lfloor\frac{1}{5}\rfloor \mod 5$, so $2 \equiv 1 + c \mod 5$ and $c = 1$. Similarly, we find that $d = 2$.
Now, we may choose any e and f such that $\gcd(cf - de, n) = 1$. Let us say that $e = 1$ and $f = 3$, so we have $\gcd(cf - de, n) = \gcd(1, 5) = 1$.
We may now continue to fill in the numbers from 2 to 24, using the uniform step method to acquire the following magic square.
For example, for $j = 11$,
$x_{11} \equiv 1 + 1(11) + (1)\lfloor\frac{11}{5}\rfloor \mod 5$
$x_{11} \equiv 1 + 11 + 1(2) \mod 5$
$x_{11} \equiv 14 \equiv 4 \mod 5$

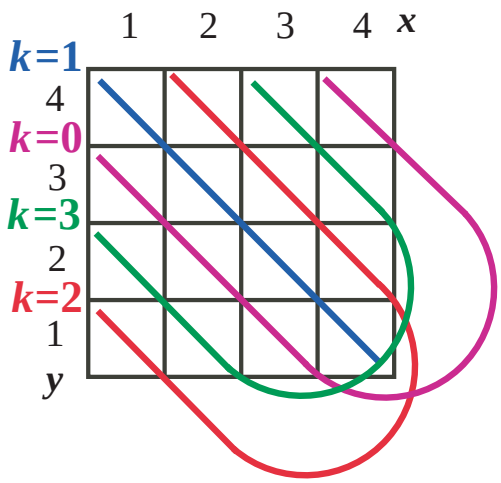
$y_{11} \equiv 1 + 2(11) + (3)\lfloor\frac{11}{5}\rfloor \mod 5$
$y_{11} \equiv 1 + 22 + 3(2) \mod 5$
$y_{11} \equiv 29 \equiv 4 \mod 5$
Therefore 11 is placed in the fourth column from the left, in the fourth row from the bottom.
After repeating this process for all numbers you will obtain the following magic square.

21	14	2	15	8
17	5	23	11	4
13	1	19	7	20
9	22	10	3	16
0	18	6	24	12

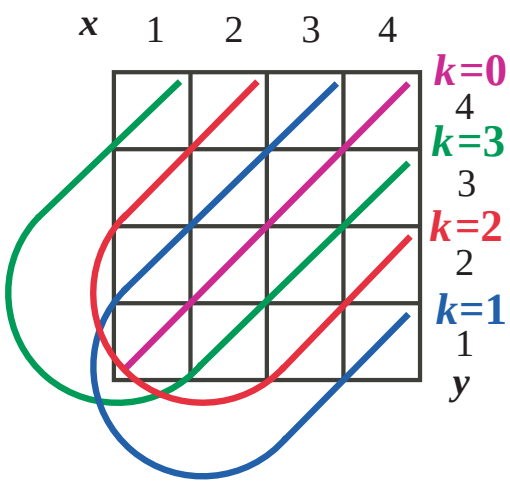
Problem:
Create your own 4×4 magic square using the uniform step method.

Diabolic Magic Squares

Defintion:
The n positive diagonals of an $n \times n$ square are given by $x + y \equiv k \mod n$.



The n negative diagonals of an $n \times n$ square are given by $y \equiv x + k \mod n$.



Definition:
An $n \times n$ magic square for which the sum of each positive and negative diagonal is the magic constant is called *diabolic*.
The following magic square is diabolic.

6	3	13	12
15	10	8	1
4	5	11	14
9	16	2	7

Multimagic Squares

Definition:
A $p-$multimagic square is an $n \times n$ square such that if you raise each element in the square by its kth power for $k = 1, 2, \ldots, p$, then the resulting squares are all magic.

There are no 3×3 multimagic squares.

Problem Set

1. Prove that $1^2 + 2^2 + \cdots + (p-1)^2 \equiv 0 \mod p$, if p is a prime greater than 3. Is it true that $1^2 + 2^2 + \cdots + (p-1)^2 \not\equiv 0 \mod p$, if $n > 3$ is not a prime?

2. Which of the following quadratic congruences have solutions?

   (a) $x^2 \equiv 4 \mod 149$

   (b) $x^2 \equiv 2 \mod 149$

   (c) $x^2 \equiv 2 \mod 151$

3. For each of the following either find all values of x that satisfy the congruence or show that the congruence has no solution.

   (a) $7x^2 + x + 11 \equiv 0 \mod 17$

   (b) $2x^2 + 7x - 13 \equiv 0 \mod 61$

4. Prove that if p is an odd prime and $\gcd(a, p) = 1$, then either $a^{\frac{p-1}{2}} \equiv 1 \mod p$ or $a^{\frac{p-1}{2}} \equiv -1 \mod p$.

5. Construct the 7×7 magic square using the uniform step method with $a = 5, b = 1, c = 1, d = -2, e = 1$, and $f = 3$. Is it diabolic?