Diary of a Mod Man

Graphing in Modular Arithmetic

UNIVERSITY OF NOTRE DAME

Modular Numbers

- Design of system
  - Finitely many integers
  - The number of integers is the *modulus*, e.g. $\mathbf{Z}_5$
  - Counting wraps around, e.g. 0, 1, 2, 3, 4, 0, 1, 2, 3, 4, 0, 1, 2, 3, 4, ...
  - Integers outside the system are replaced, e.g. $12 \equiv 2 \pmod 5$ or $-6 \equiv 4 \pmod 5$
- Often called “clock” numbers
  - Normal clocks have an hour modulus of 12 and a minute and second modulus of 60
  - Military time has hour modulus of 24
  - Some people are proponents of a 10-hour day

UNIVERSITY OF NOTRE DAME

Modular Arithmetic

- Addition
  - What is 7 + 9 (mod 12)?
    - Compare to normal clock: “On a 12-hour clock, start at 7 and count forward 9. What time is it?”
    - Answer: 7 + 9 = 16 ≡ 4 (mod 12)
  - What is 7:24 + 9:53 (mod 12:60)?
    - Compare to normal clock: “On a 12-hour:60-minute clock, start at 7:24 and count forward 9:53. What time is it?
    - Answer: 7:24 + 9:53 = 16:77 ≡ 17:17 ≡ 5:17 (mod 12:60)
    - This is non-trivial to think about, and more cumbersome to write, so is it any wonder children have trouble mastering the clock?
  - Subtraction is defined, e.g. 7 – 9 ≡ 10 (mod 12)

UNIVERSITY OF NOTRE DAME

Modular Arithmetic

- Multiplication
  - What is $10 \cdot 3 \pmod{12}$?
    - Compare to normal clock: “On a 12-hour clock, start at 10 and triple that time. What time is it?”
    - Answer: $10 \cdot 3 = 30 \equiv 6 \pmod{12}$
  - What is $10{:}24 \cdot 3 \pmod{12{:}60}$?
    - Compare to normal clock: “On a 12-hour:60-minute clock, start at 10:24 and triple that time. What time is it?
    - Answer: $10{:}24 \cdot 3 = 30{:}72 \equiv 31{:}12 \equiv 7{:}12 \pmod{12{:}60}$
  - Division is NOT necessarily defined because the divisor may not have a multiplicative inverse in the system, e.g. $10 \div 3 \equiv (10 + 12n) \div 3$ has no integer solution

UNIVERSITY OF NOTRE DAME

Modular Algebra

- Applying the rules of normal algebra to a modular system at first seems normal
  - Solve: $x + 4 \equiv 9 \pmod{12}$
    - $x + 4 \equiv 9 \rightarrow x \equiv 5$
  - Solve: $5x + 4 \equiv 9 \pmod{12}$
    - $5x + 4 \equiv 9 \rightarrow 5x \equiv 5 \rightarrow x \equiv 1$

Modular Algebra

- But, because division may be involved, some results can be unexpected
  - Solve: $4x + 3 \equiv 11 \pmod{12}$
    - $4x + 3 \equiv 11 \rightarrow 4x \equiv 8 \rightarrow x \equiv 2$
    - $4x + 3 \equiv 11 \rightarrow 4x \equiv 8 \rightarrow 4x \equiv 20 \rightarrow x \equiv 5$
    - $4x + 3 \equiv 11 \rightarrow 4x \equiv 8 \rightarrow 4x \equiv 32 \rightarrow x \equiv 8$
    - $4x + 3 \equiv 11 \rightarrow 4x \equiv 8 \rightarrow 4x \equiv 44 \rightarrow x \equiv 11$

Modular Algebra

- In the previous two problems, the unique solution was obtained when dividing by a number relatively prime to the modulus
- This implies that not every fraction is possible in a modulus that is not prime
  - In mod 12: 1/1, 1/5, 1/7, and 1/11 are possible while 1/2, 1/3, 1/4, 1/6, 1/8, 1/9, 1/10 aren't

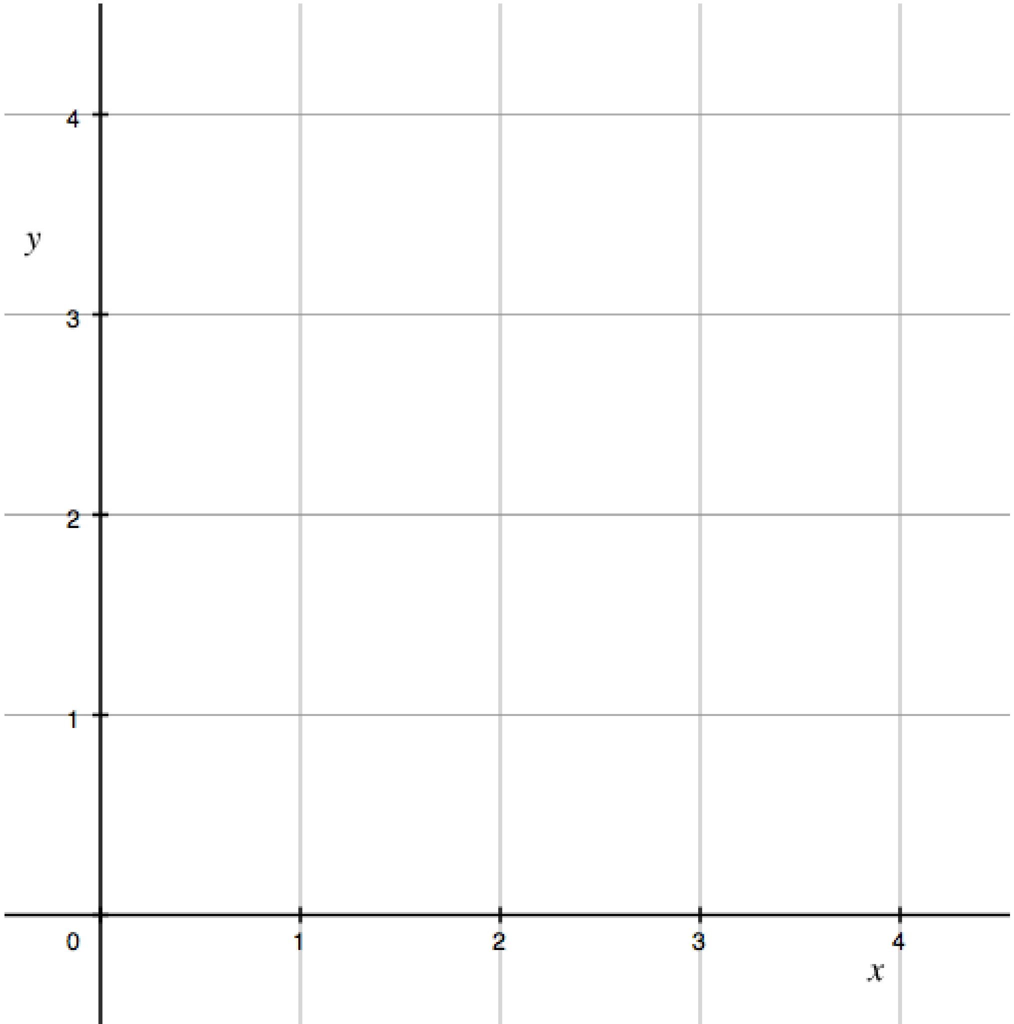
UNIVERSITY OF NOTRE DAME

Modular Functions

- Notation
  - Instead of $f(x)$, let $f_m(x)$ indicate a function in mod m. This notation is chosen to mirror the fact that we are working in $\mathbf{Z}_m$.
    - o $f_{12}(x) = 5x + 4$ is equivalent to $y \equiv 5x + 4 \pmod{12}$
- Graphing
  - Instead of the normal four-quadrant system, we need only QI, specifically $\mathbf{Z}_m$ x $\mathbf{Z}_m$.

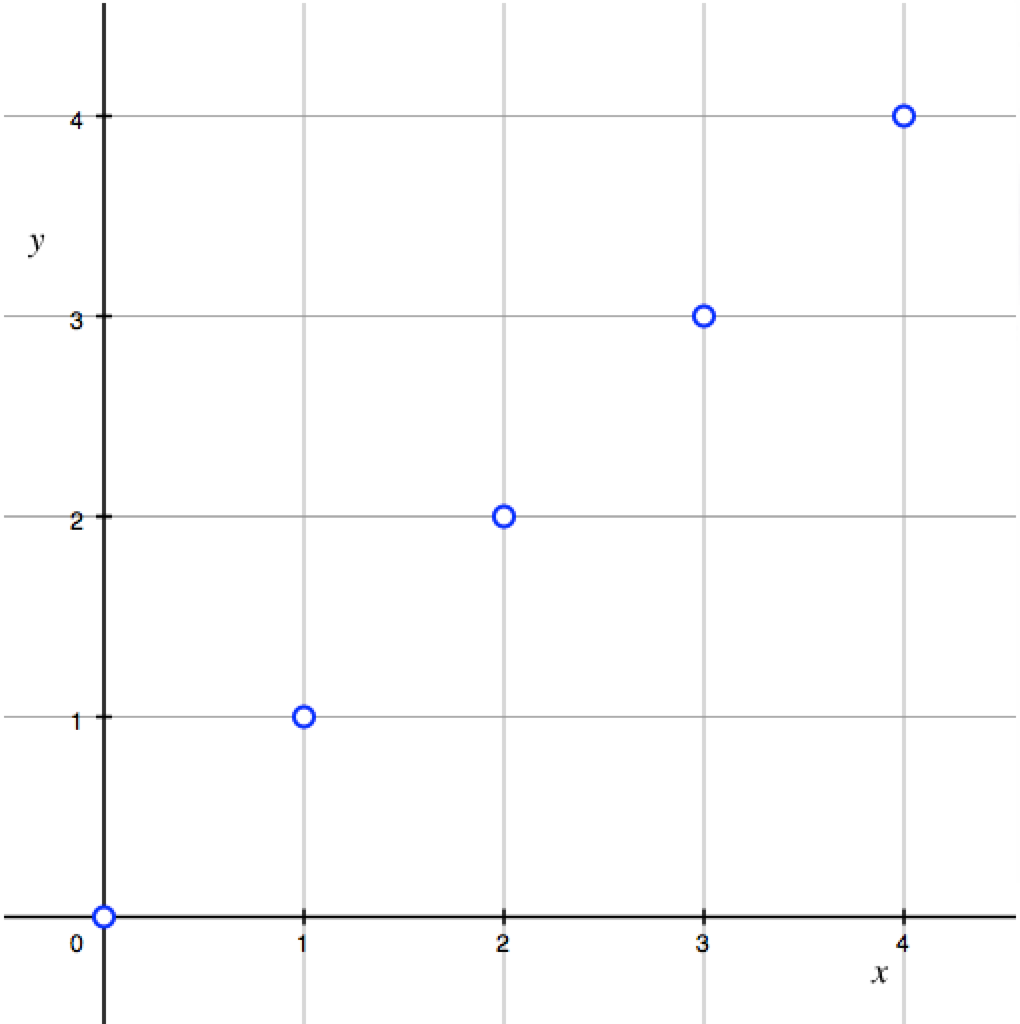
Modular Functions

- Examine graphs of function in $\mathbf{Z}_5$.



Modular Functions

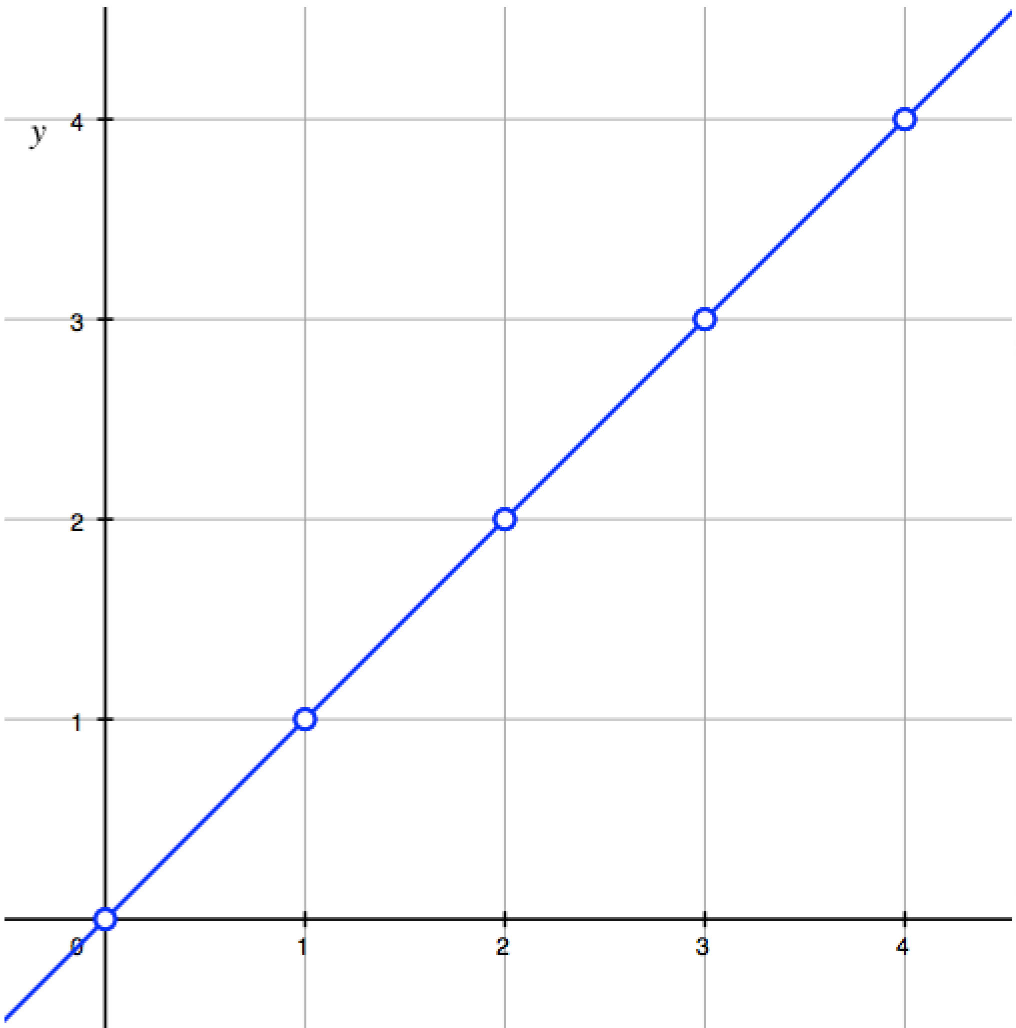
- $f_5(x) \equiv x$



UNIVERSITY OF NOTRE DAME

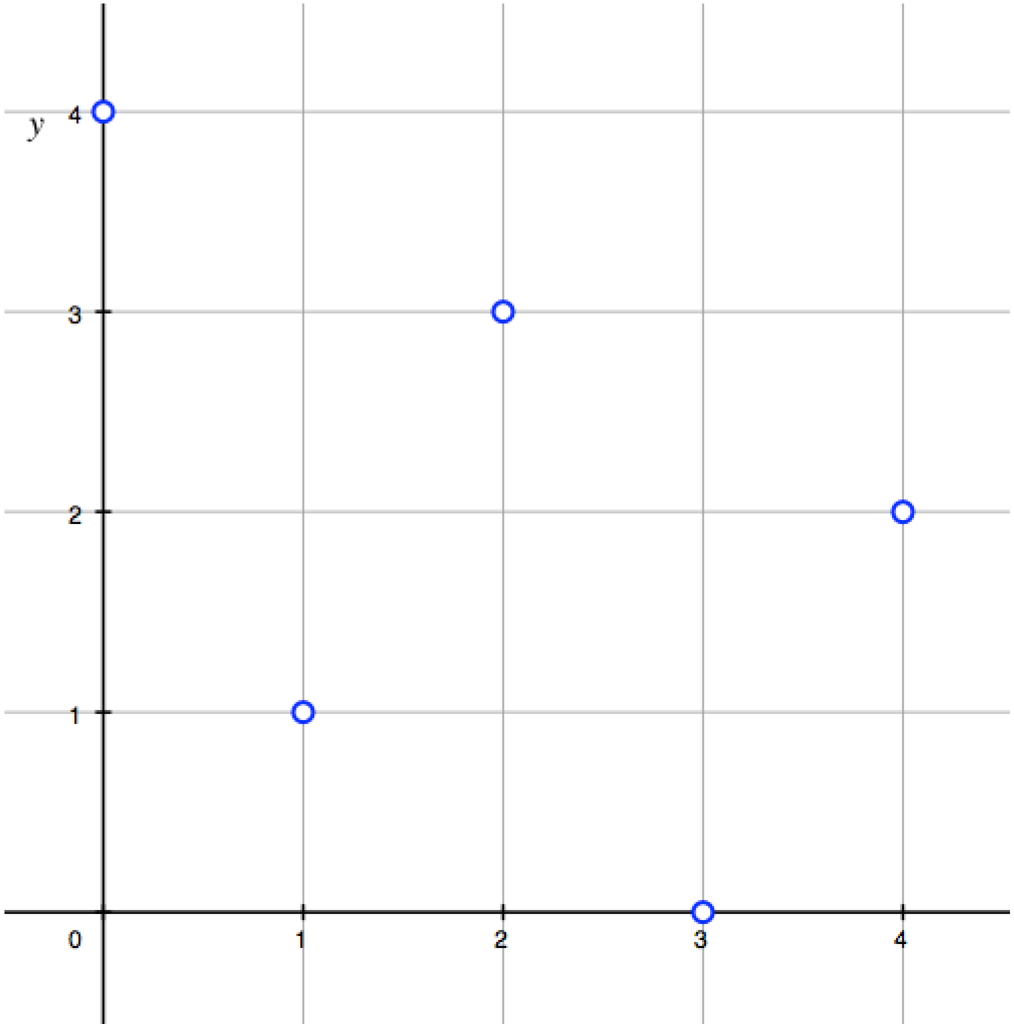
Modular Functions

- Compare to $f(x) = x$



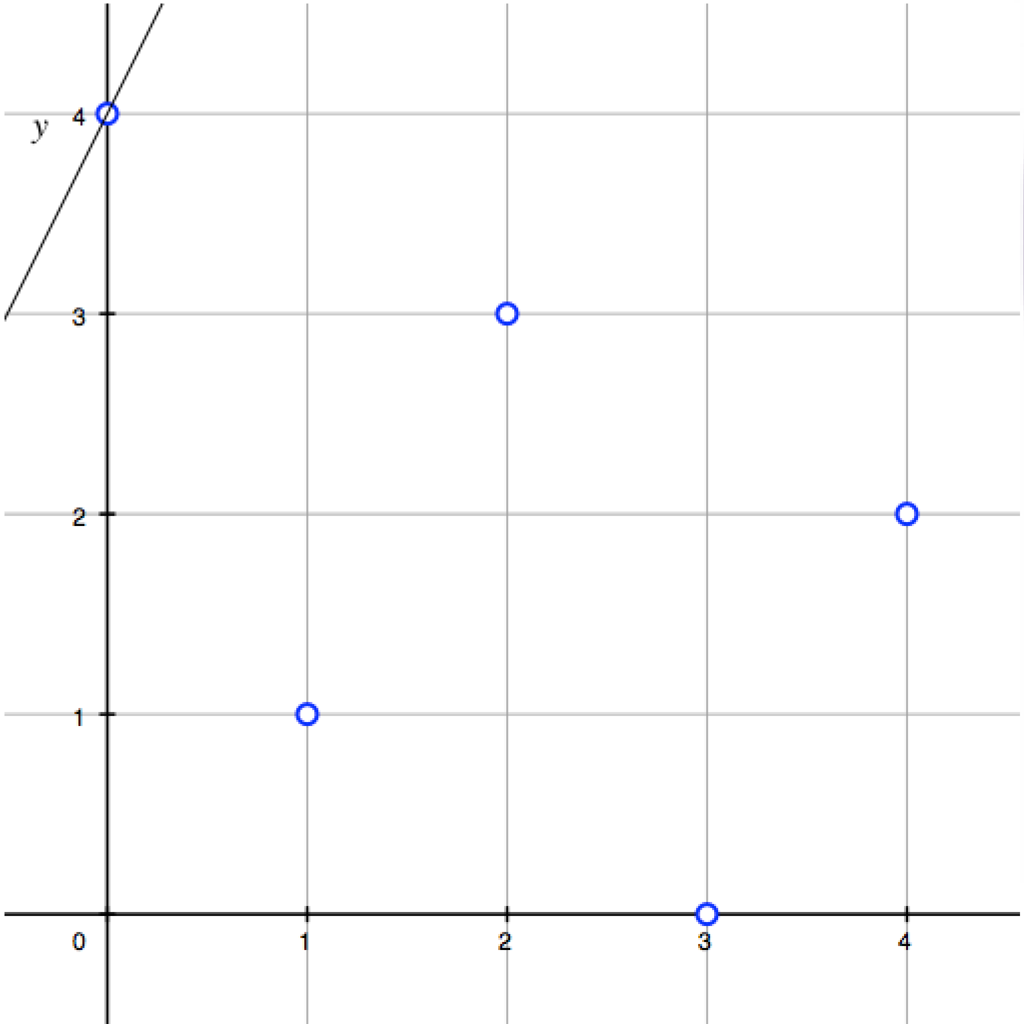
Modular Functions

- $f_5(x) \equiv 2x + 4$



Modular Functions

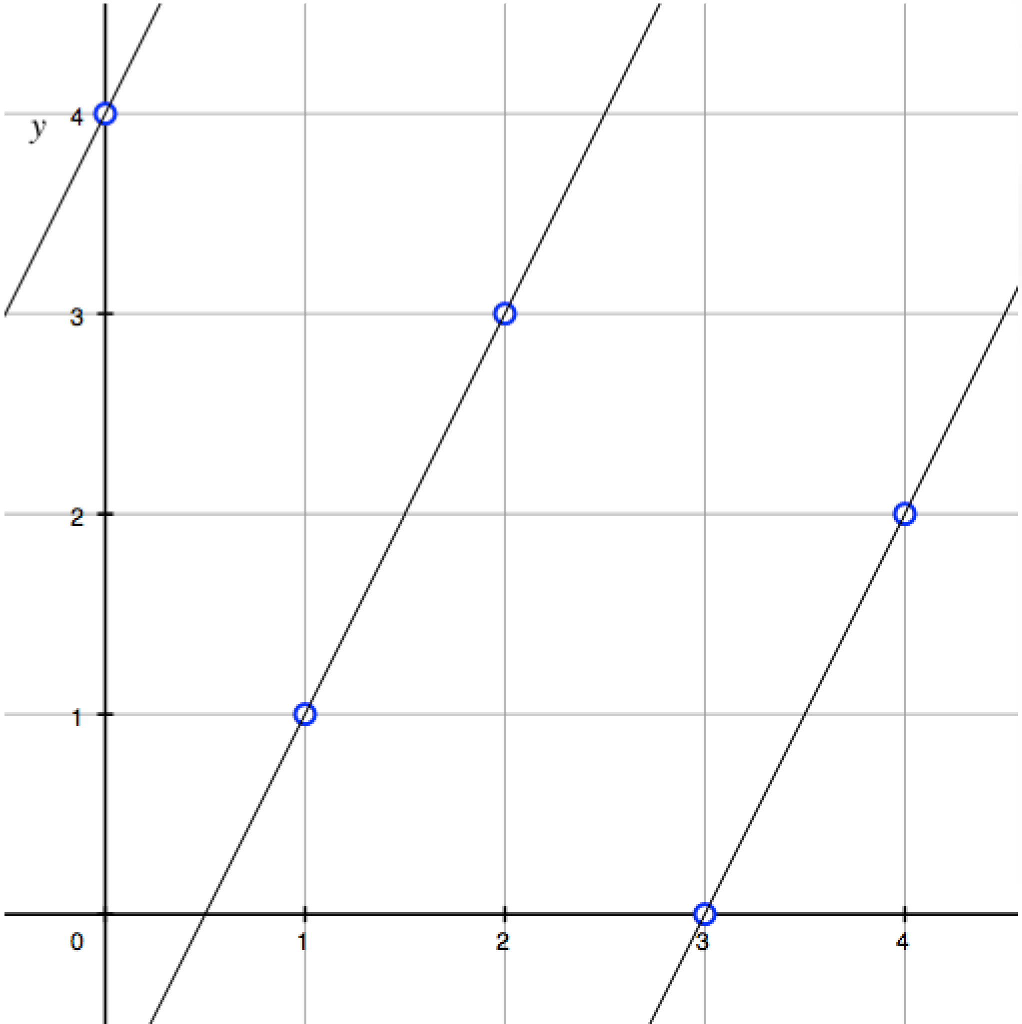
- Compare to $f(x) = 2x + 4$



UNIVERSITY OF NOTRE DAME

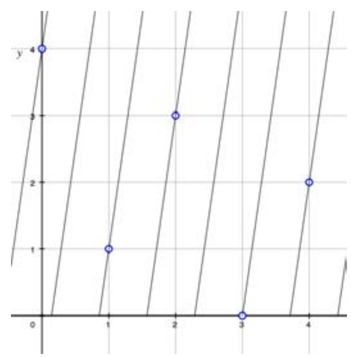
Modular Functions

- Include $f(x) = 2x - 1$ and $f(x) = 2x - 6$

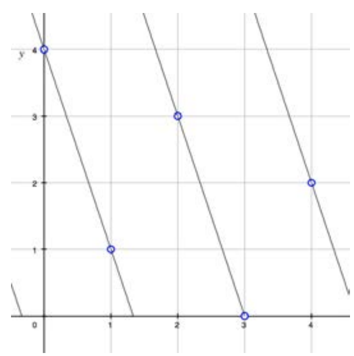


Modular Functions

- Theoretically, $f_5(x) \equiv 2x + 4$ could be modeled by any line with slope $m \equiv 2$ and any y-intercept $b \equiv 4$
  - $f_5(x) \equiv 7x - 1$

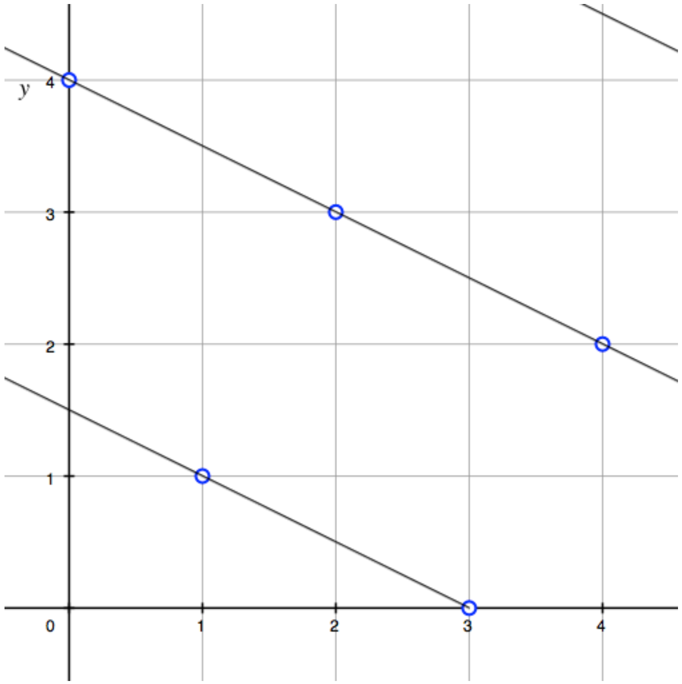


  - $f_5(x) \equiv -3x + 9$



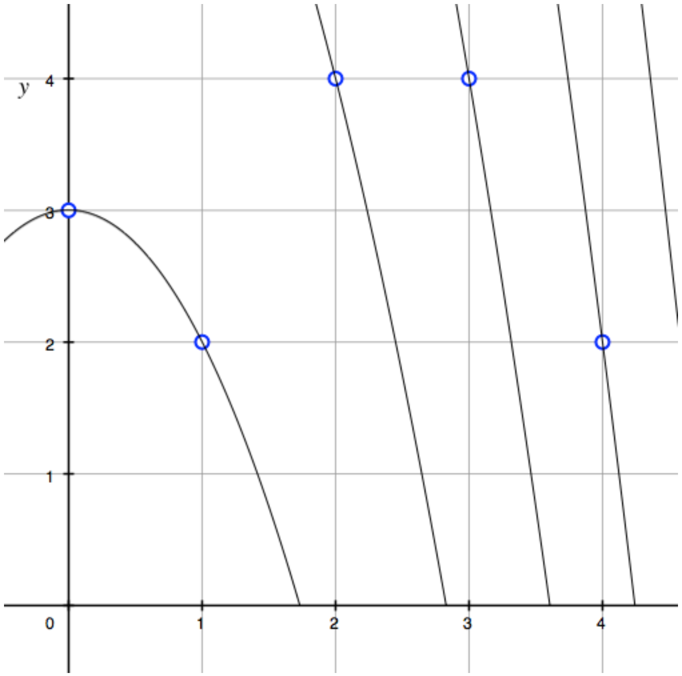
Modular Functions

- Theoretically, $f_5(x) \equiv 2x + 4$ could be modeled using fractions defined within $\mathbf{Z}_5$ as well
  - $f_5(x) \equiv -\frac{1}{2}x + 4$

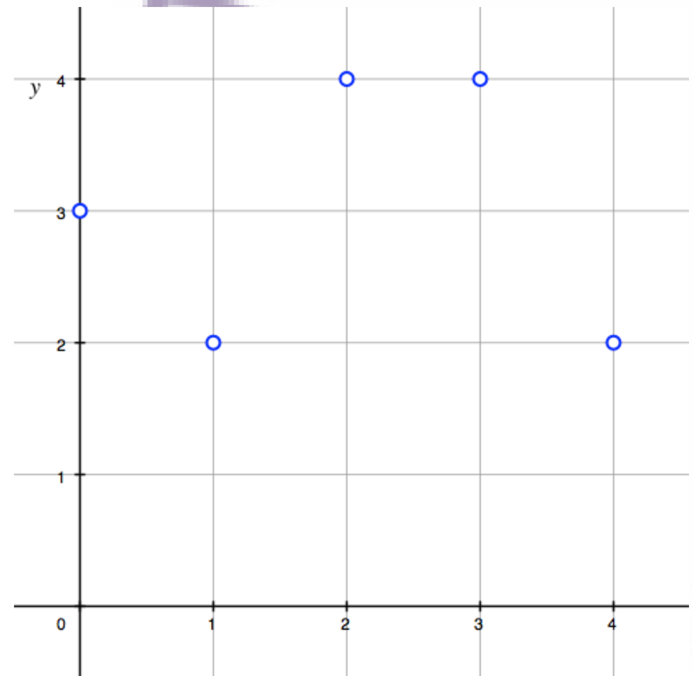


Modular Functions

- $f_5(x) \equiv 3 - x^2$

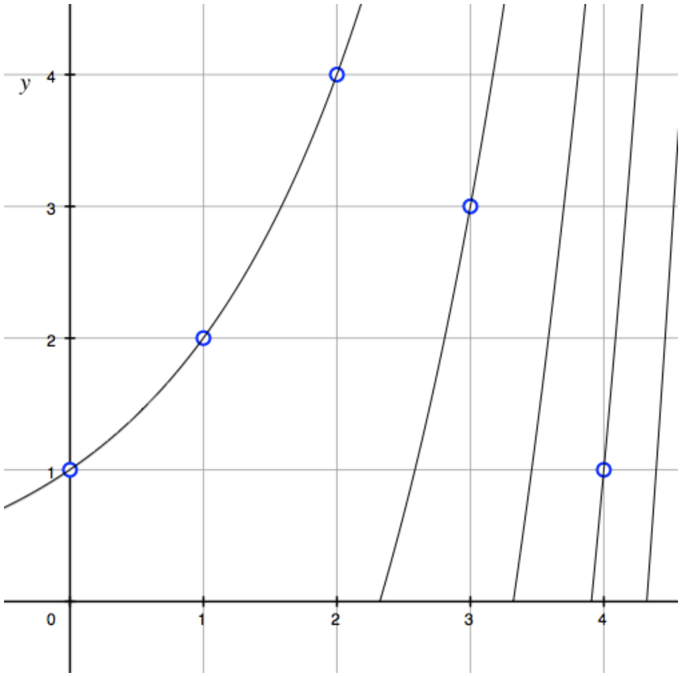


→

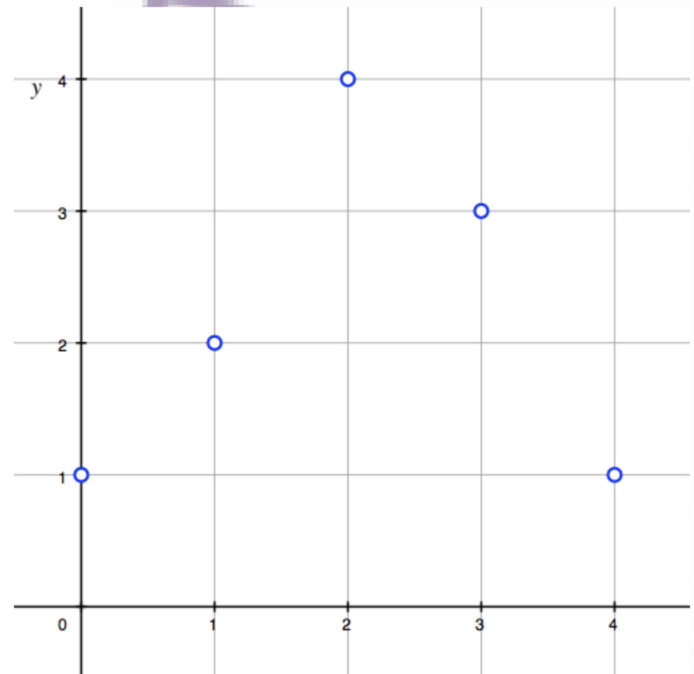


Modular Functions

- $f_5(x) \equiv 2^x$

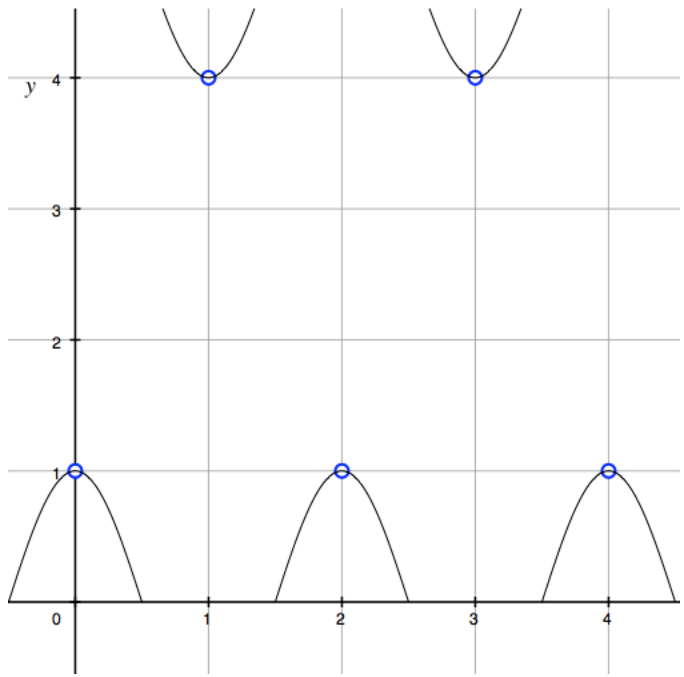


→

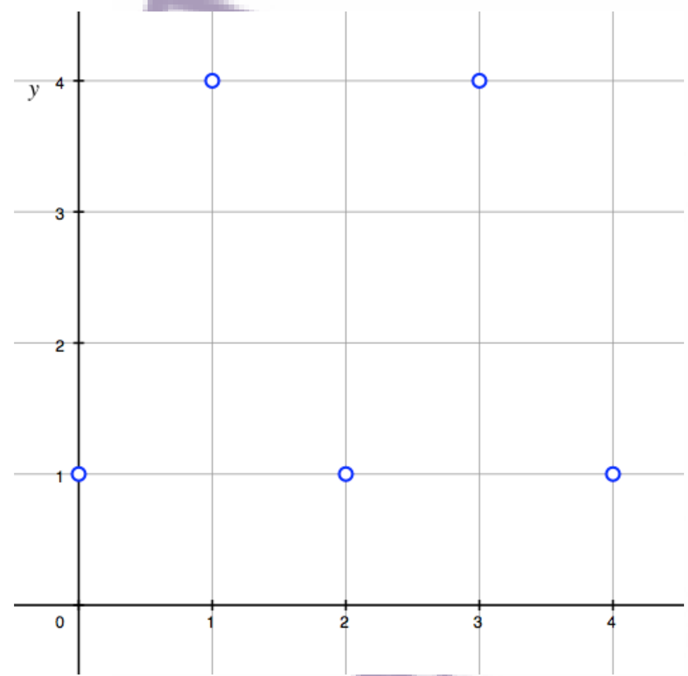


Modular Functions

- $f_5(x) \equiv \cos \square x$

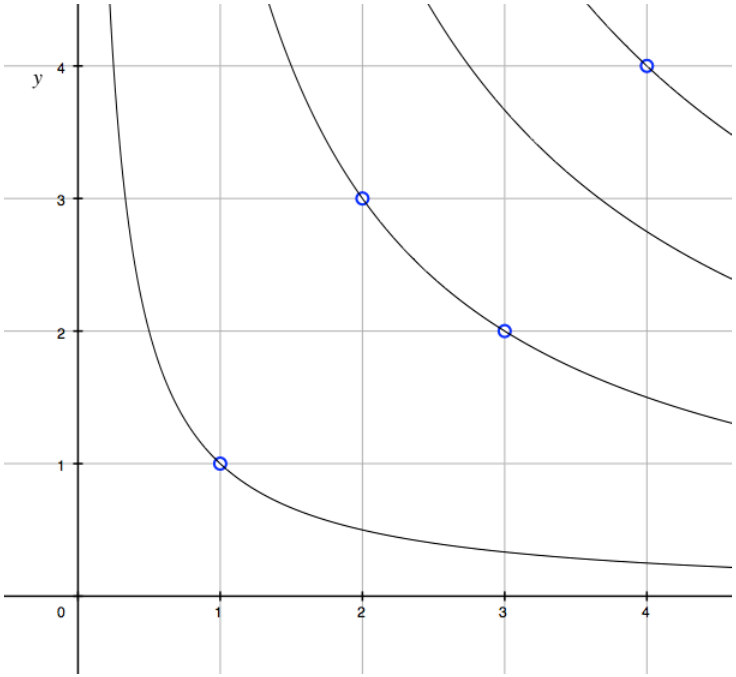


→

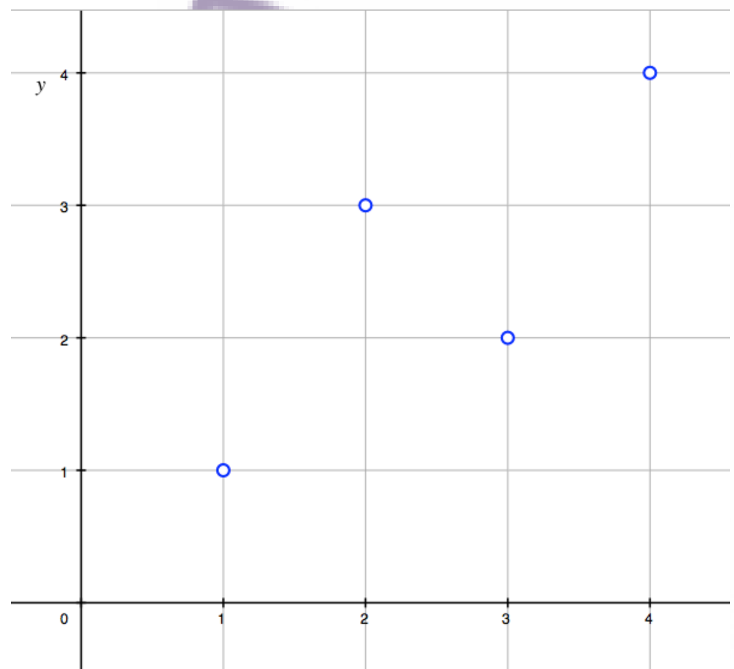


Modular Functions

- $f_5(x) \equiv 1/x$

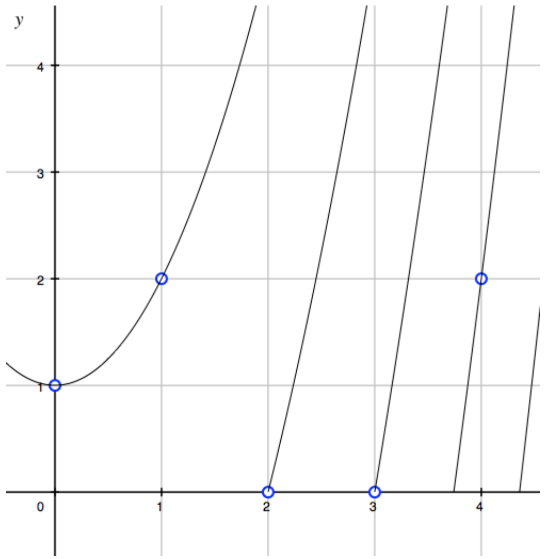


→



Modular Algebra

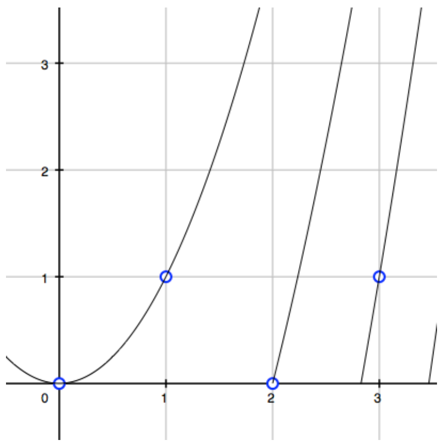
- Can factoring be used?
  - Solve graphically: $x^2 - 4 \equiv 0 \pmod 5$
    - o $x^2 - 4 \equiv 0 \rightarrow x \equiv 2$ or $x \equiv 3$



  - Solve algebraically: $x^2 - 4 \equiv 0 \pmod 5$
    - o $x^2 - 4 \equiv 0 \rightarrow (x + 2)(x - 2) \equiv 0 \rightarrow x \equiv \pm 2 \rightarrow x \equiv 2$ or $x \equiv 3$

Modular Algebra

- ...But when modulus is not prime, can it still be used?
  - Solve graphically: $x^2 - 4 \equiv 0 \pmod 5$
    - $x^2 - 4 \equiv 0 \rightarrow x \equiv 0$ or $x \equiv 2$



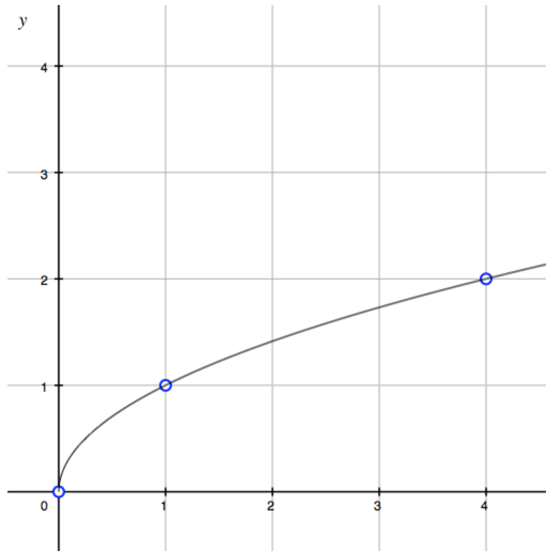
  - Solve algebraically: $x^2 - 4 \equiv 0 \pmod 4$
    - $x^2 - 4 \equiv 0 \rightarrow x^2 \equiv 0 \rightarrow x \equiv 0$
    - $x^2 - 4 \equiv 0 \rightarrow (x + 2)(x - 2) \equiv 0 \rightarrow x \equiv \pm 2 \rightarrow x \equiv 2$

Modular Algebra

- The Zero Product property is not true in all modular systems
  - For $\mathbf{Z}$, $xy = 0 \rightarrow x = 0$ or $y = 0$
  - For $\mathbf{Z}_5$, $xy \equiv 0 \rightarrow x \equiv 0$ or $y \equiv 0$
  - However, for $\mathbf{Z}_4$, $xy \equiv 0 \rightarrow x \equiv 0$ or $y \equiv 0$ is false, since $x \equiv y \equiv 2$ is another solution

Modular Algebra

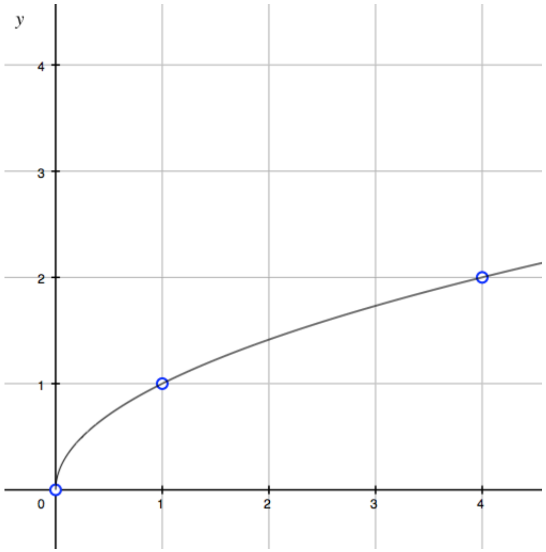
- Can squaring be used?
  - Solve graphically: $\sqrt{x} \equiv 1 \pmod{5}$
    - o $\sqrt{x} \equiv 1 \rightarrow x \equiv 1$



  - Solve algebraically: $\sqrt{x} \equiv 1 \pmod{5}$
    - o $\sqrt{x} \equiv 1 \rightarrow x \equiv 1$

Modular Algebra

- ...But the domain of the square root function in $\mathbf{Z}_5$ is not $\mathbf{Z}_5$
  - $\sqrt{2}$ and $\sqrt{3}$ are not defined because $x^2 \equiv 2$ and $x^2 \equiv 3$ have no solution

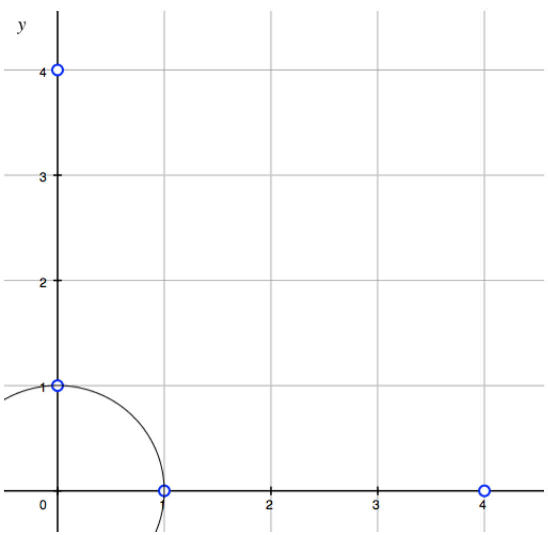


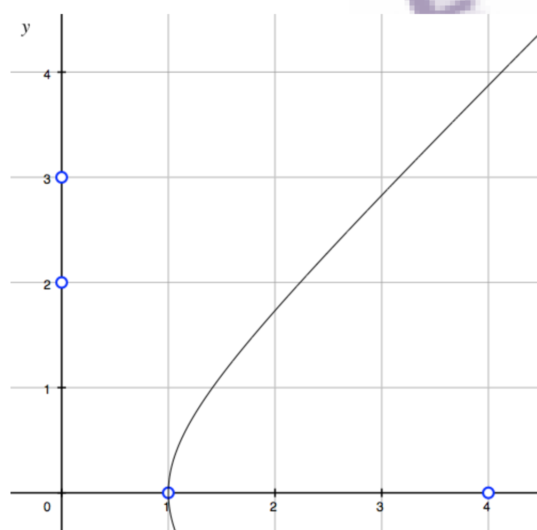
Modular Algebra

- The only operations that can be used in $\mathbf{Z}_5$ are operations that act cyclic on the elements of $\mathbf{Z}_5$
  - That is to say, the operation must be a bijection (one-to-one and onto) between the elements of the domain and the range
  - Addition, multiplication are both cyclic on $\mathbf{Z}_p$
  - Note that none of squaring, square rooting, exponentials, cosines, nor most other functions turn out to be cyclic

Further Exploration

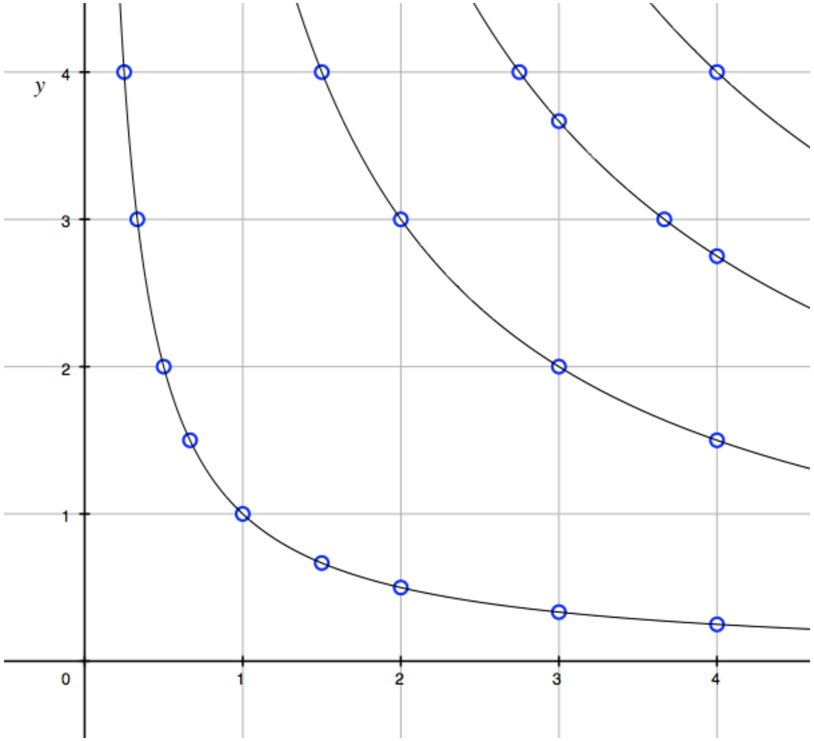
- What about graphs of relations, such as conic sections?
  - Parabola: $y^2 \equiv x \pmod 5$
    - o As might be expected, this works out to be identical to the square root function
  - Circle/ellipse: $x^2 + y^2 \equiv 1 \pmod 5$
  - Hyperbola: $x^2 - y^2 \equiv 1 \pmod 5$





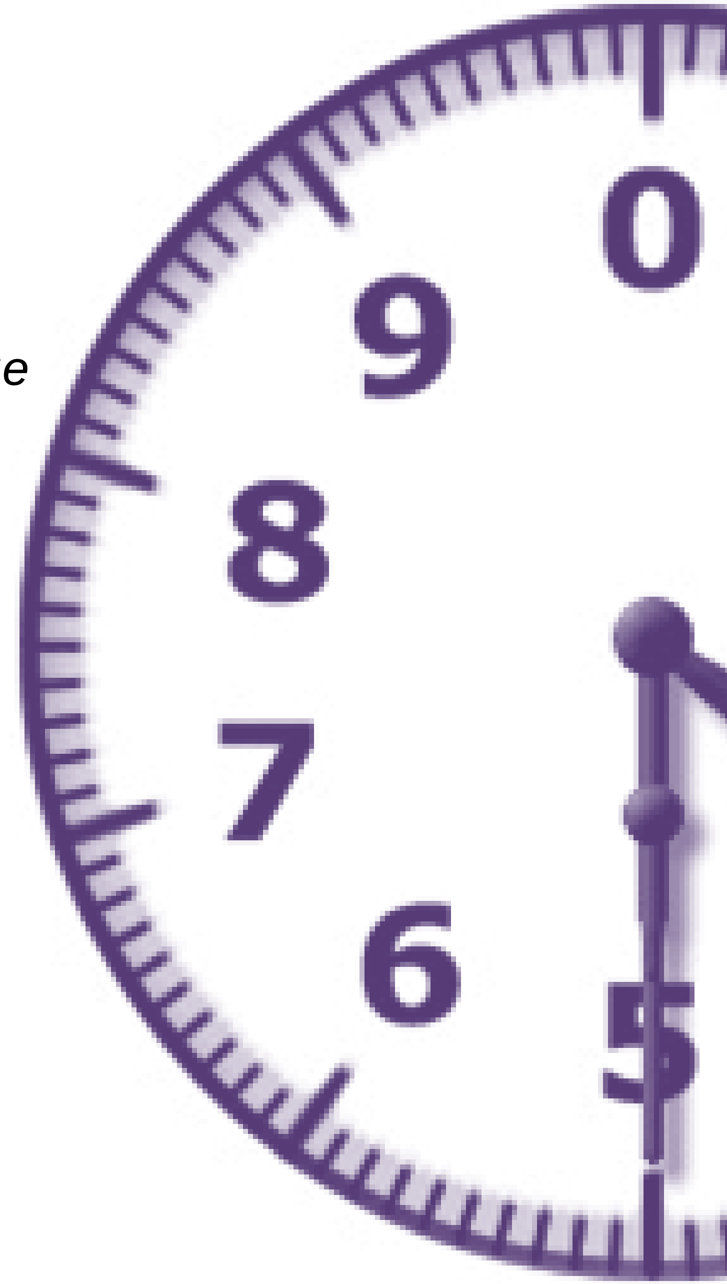
Further Exploration

- Since fractions are possible, why confine to integer points?
  - $f_5(x) \equiv 1/x$



Works Cited

Bird, Marion H. “A New Look at Functions in Modular Arithmetic” *The Mathematical Gazette* Jun 1980: 78-86. Print.



UNIVERSITY OF NOTRE DAME

RET@ND

Participant

Ben Dillon

(Saint Joseph HS)

Adviser

Nicole Kroeger

(University of Notre Dame)

UNIVERSITY OF NOTRE DAME