Number Theory with python PROGRAMMING

Number Theory Games

Lecture 10

Justin Stevens

Outline

1. Number Theory Games
   - TAG_5
   - Divisors of 60 Game
   - Nim
   - Fibonacci Nim
2. Euclidean Algorithm Revisited
3. Parting Shots

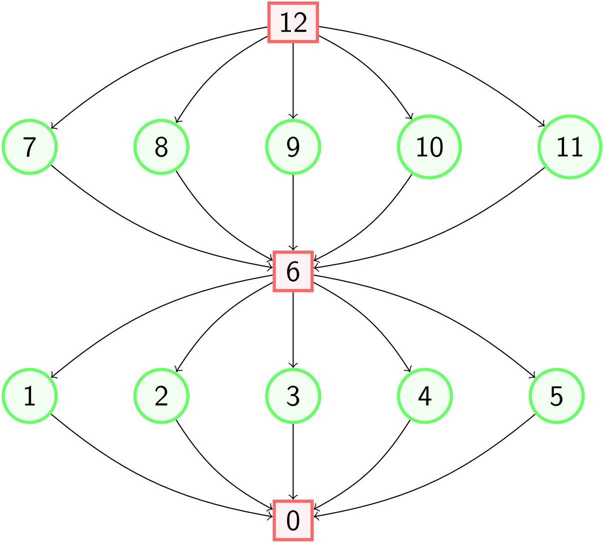
TAG_5 Rules

Consider the take-away game TAG_5 below:

> *Let there be n chips on the table and A, B be two players, A making the first move. Each player may in turn take-away either $1, 2, 3, 4,$ or 5 chips from the pile. The winner is the player who removes the final chip(s), leaving none for the other player.*

- Play TAG_5 for $n = 42$. Who has the winning strategy?
- Play TAG_5 for $n = 50$. Who has the winning strategy?
- For a general n, does player A or player B have the winning strategy?

TAG_5 Analysis



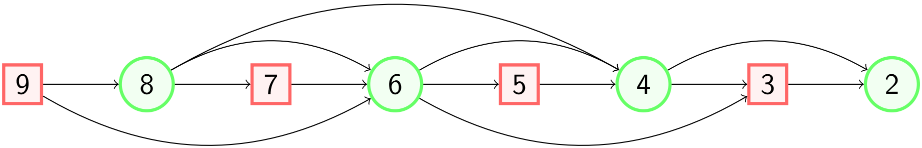
Reducing by Divisors Game

Consider the variation of the take-away game below:

> *Let there be* 60 *chips on the table and* A, B *be two players,* A *making the first move. Each player in turn generates new numbers by subtracting a positive proper divisor from the current sum. The winner is the player who makes the new number* 1.

Does player A or player B have the winning strategy?

Divisors Game Analysis



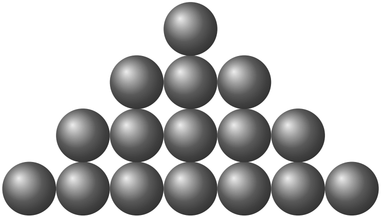
Nim

Consider the rules for the following game, known as Nim:

> *There are four piles of stones of size* $1, 3, 5,$ *and* 7*. Players A and B alternate choosing a pile and taking at least one stone from that pile. The game continues until there are no stones remaining.*

There are two variations on the winning condition:

- **Normal Play:** The player to take the last stone wins.
- **Misère Play:** The player to take the last stone loses.



Nim-Sum Definition

Definition. The nim-sum of two numbers a and b is denoted $a \oplus b$. To form this, write the two numbers in binary and add without carry:

$$0 \oplus 0 = 1 \oplus 1 = 0 \text{ and } 0 \oplus 1 = 1 \oplus 0 = 1.$$

The operation is also known as “exclusive or" (xor).

For piles of size $1, 3, 5$, and 7, consider the table below:

	2^2	2^1	2^0
1	0	0	1
3	0	1	1
5	1	0	1
7	1	1	1
	0	0	0

Therefore, $1 \oplus 3 \oplus 5 \oplus 7 = 0$. When the nim-sum is 0, we call a position *balanced*. Otherwise, it is *unbalanced*.

Example. Compute $5 \oplus 6 \oplus 7$ and $9 \oplus 10 \oplus 15$.

Nim-Sum Examples

Example. Compute $5 \oplus 6 \oplus 7$ and $9 \oplus 10 \oplus 15$.

	2^2	2^1	2^0
5	1	0	1
6	1	1	0
7	1	1	1
	1	0	0

Therefore, $5 \oplus 6 \oplus 7 = 4$. To make the position balanced, we remove 4 from any pile. Then,

$$1 \oplus 6 \oplus 7 = 5 \oplus 2 \oplus 7 = 5 \oplus 6 \oplus 3 = 0.$$

	2^3	2^2	2^1	2^0
9	1	0	0	1
10	1	0	1	0
15	1	1	1	1
	1	1	0	0

Therefore, $9 \oplus 10 \oplus 15 = 10$. To make the position balanced, we remove 4 from one of the first two piles, or 12 from the last pile:

$$5 \oplus 10 \oplus 15 = 9 \oplus 6 \oplus 15 = 9 \oplus 10 \oplus 3 = 0.$$

Winning Strategy

The practical strategy to win at the game of *Nim* is for a player to get the other into one of the following positions:

2 Heaps	3 Heaps	4 Heaps
2 2	1 2 3	1 1 n n
3 3	1 4 5	1 2 4 7
4 4	1 6 7	1 2 5 6
5 5	1 8 9	1 3 4 6
6 6	2 4 6	1 3 5 7
7 7	2 5 7	2 3 4 5

For Misére Nim, only the last move changes. In particular,

- Play exactly like you would in normal play until your opponent leaves one pile of size greater than one.
- At this point, reduce this pile to size 1 or 0, whichever leaves an odd number of piles with only one object.

Misére Nim Example

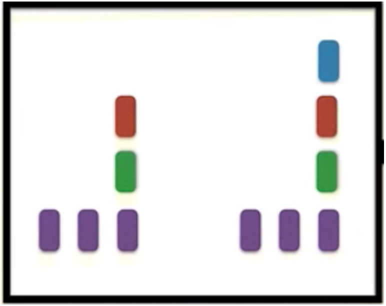


Figure 1: Mathologer

Proof of Winning Strategy in Nim

Theorem. (Charles Bouton) In a normal Nim game, the player making the first move has a winning strategy if and only if the nim-sum of the sizes of the heaps is nonzero. Otherwise, the second player has a winning strategy.

Proof. Notice that the nim-sum ($\oplus$) obeys the usual associative and commutative laws of addition and also satisfies the property $x \oplus x = 0$.

Let $x_1, \cdots, x_n$ be the size of the heaps before a move, and $y_1, \cdots, y_n$ be the corresponding sizes after. Let $s = x_1 \oplus \cdots \oplus x_n$ and $t = y_1 \oplus \cdots \oplus y_n$. If the move was in heap k, we have $x_i = y_i$ for all $i \neq k$, and $x_k > y_k$. Then,

$$\begin{aligned} t &= 0 \oplus t \\ &= s \oplus s \oplus t \\ &= s \oplus (x_1 \oplus \cdots \oplus x_n) \oplus (y_1 \oplus \cdots \oplus y_n) \\ &= s \oplus (x_1 \oplus y_1) \oplus \cdots \oplus (x_n \oplus y_n) \\ &= s \oplus 0 \oplus \cdots \oplus 0 \oplus (x_k \oplus y_k) \oplus 0 \oplus \cdots \oplus 0 \\ &= s \oplus x_k \oplus y_k. \end{aligned}$$

Proof of Winning Strategy in Nim Continued

We've proven that if there is a move in heap k, then $t = s \oplus x_k \oplus y_k$.

Lemma. If $s = 0$, then $t \neq 0$ no matter what move is made.

Proof.

If there are no moves, then the lemma is vacuously true. Otherwise, any move in heap k produces $t = x_k \oplus y_k$, which is nonzero since $x_k \neq y_k$. □

Lemma. If $s \neq 0$, then it is possible to make a move so that $t = 0$.

Proof.

Let d be the position of the leftmost nonzero bit in the binary form of s, and choose k such that the dth bit of x_k is also nonzero. Let $y_k = s \oplus x_k$.

Since bit d decreases from 1 to 0 and any change in the remaining bits is at most $2^d - 1$, the first player can take $x_k - y_k$ stones from heap k. Then,

$$t = s \oplus x_k \oplus y_k = s \oplus x_k \oplus (s \oplus x_k) = 0.$$

□

Fibonacci Nim

Consider the rules for the following game, known as Fibonacci Nim:

> *Let there be n chips on the table and A, B be two players who alternate removing chips from the pile. On the first move, a player is not allowed to take all of the coins, and on each subsequent move, the number of coins removed can be any number that is at most twice the previous move. The winner is the player who removes the final chip(s), leaving none for the other player.*

- Play Fibonacci nim for $n = 140$. Who has the winning strategy?
- Play Fibonacci nim for $n = 144$. Who has the winning strategy?
- For a general n, does player A or player B have the winning strategy?

Example. (Zeckendorf's Theorem) Prove that every positive integer N can be represented as the unique sum of non-consecutive Fibonacci numbers. In other words, there exists a unique $\{a_j\}_{j=0}^{m}$ such that

$$N = \sum_{j=0}^{m} F_{a_j}, \quad a_0 \geq 2 \text{ and } a_{j+1} > a_j + 1.$$

Fibonacci Sum Existence

Proof by Strong Induction.

For the base case $N = 1$, the unique representation is $1 = F_2$. Now, assume that every every integer up to K can be written as the unique sum of distinct non-consecutive Fibonacci numbers. Let F_a be the largest Fibonacci number such that $F_a \leq K + 1$. If $F_a = K + 1$, then we are clearly done. Otherwise, $F_a < K + 1 < F_{a+1}$, therefore

$$0 < (K + 1) - F_a < F_{a+1} - F_a = F_{a-1}. \qquad (\star)$$

By our hypothesis, there exists a sequence $\{a_j\}_{j=0}^{m}$ with $a_{j+1} > a_j + 1$ and

$$K + 1 = F_a + \sum_{j=0}^{m} F_{a_j}.$$

Since $m > a + 1$ by $(\star)$, we have found a representation for $K + 1$. $\square$

Fibonacci Sum Uniqueness

Lemma

The sum of any set of distinct, non-consecutive Fibonacci numbers whose largest member is F_j is strictly less than the next Fibonacci number F_{j+1}.

For the sake of contradiction, assume we have two representations:

$$K + 1 = F_{a_1} + F_{a_2} + \cdots + F_{a_m} = F_{b_1} + F_{b_2} + \cdots + F_{b_l}.$$

WLOG assume that $a_m \geq b_l$. If $a_m > b_l$, by our Lemma,

$$\begin{aligned} K + 1 = F_{b_1} + F_{b_2} + \cdots + F_{b_l} &< F_{b_l+1} - 1 \\ &\leq F_{a_m} - 1 \\ &< F_{a_1} + F_{a_2} + \cdots + F_{a_m} \\ &= K + 1. \end{aligned}$$

Therefore $a_m = b_l$. By our hypothesis, $K + 1 - F_{a_m} = K + 1 - F_{b_l}$ has a unique representation, therefore, $K + 1$ also has a unique representation.

Fibonacci Nim Strategy

Theorem. When there is a Fibonacci number of chips in the starting pile, the position is losing for the first player. Otherwise, the first player can win.

Proof. We describe the optimal strategy in Fibonacci nim in terms of the "quota" q (the maximum number of coins that can currently be removed) and the Zeckendorf representation. In particular,

- A given position is losing when q is less than the smallest Fibonacci number in the representation.
- In a winning position, it is always a winning move to remove all the coins (if this is allowed) or otherwise to remove a number of coins equal to the smallest Fibonacci number in the representation.

When this is possible, the opposing player will necessarily be faced with a losing position, because the new quota will be smaller than the smallest Fibonacci number in the Zeckendorf representation of the remaining chips.

Sprague-Grundy theorem

Figure 2: In combinatorial game theory, the Sprague-Grundy theorem states that every impartial game under the normal play convention is equivalent to a nimber.

Outline

The Game of Euclid

A third variation is a two-player game called *The Game of Euclid*:

> *Let (p, q) be a pair of positive integers satisfying $p > q$ and let A, B be two players, A making the first move. Each player may in turn subtract as many times the smaller of the remaining integers from the larger without making the result negative. The winner is the player who discovers the highest common factor of p and q, that is, by the Euclidean algorithm, the player who reduces one of the factors to zero. [Cole and Davie, 1969]*

The game has a winning strategy utilizing the golden ratio, $\varphi = 1.618\ldots$.

$$(162, 100) \xrightarrow{A} (100, 62) \xrightarrow{B} (62, 38) \xrightarrow{A} (38, 24) \xrightarrow{B} (24, 14) \xrightarrow{A} (14, 10) \xrightarrow{B} (10, 4) \xrightarrow{A} (6, 4) \xrightarrow{B} (4, 2) \xrightarrow{\boldsymbol{A}} (2, 0)$$

$$(161, 100) \xrightarrow{A} (100, 61) \xrightarrow{B} (61, 39) \xrightarrow{A} (39, 22) \xrightarrow{B} (22, 17) \xrightarrow{A} (17, 5) \xrightarrow{B} (7, 5) \xrightarrow{A} (5, 2) \xrightarrow{B} (3, 2) \xrightarrow{A} (2, 1) \xrightarrow{\boldsymbol{B}} (1, 0).$$

A wins the first game, while B wins the second. Observe $1.62 > \varphi > 1.61$.

Properties of the Game of Euclid

Example. For starting position (n, m), the Game of Euclid has properties:

(1) The ending state of the game is $(\gcd(n, m), 0)$.
(2) For $1 < a/b < \varphi$, the only move is $(a, b) \to (b, a')$, where $b/a' > \varphi$.

Proof.

(1) For the move $(n, m) \to (n - sm, m)$, by the Euclidean algorithm, $\gcd(n, m) = \gcd(n - sm, m)$. Therefore, each move preserves the gcd. Furthermore, each move reduces one of the two numbers. Since negative integers are not permitted, the ending state of the game is $(\gcd(n, m), 0)$.

(2) Since $b < a < b\varphi < 2b$, the only possible move is $(a, b) \to (b, a - b)$. Hence $a' = a - b$. Furthermore, $\varphi^2 - \varphi = 1$, so

$$\frac{b}{a'} = \frac{b}{a - b} = \frac{1}{a/b - 1} > \frac{1}{\varphi - 1} = \varphi.$$

□

Winning Strategy of the Game of Euclid

Theorem. Player A may force a win if $n/m = 1$ or if $n/m > \varphi$.

Proof by Infinite Descent.

When $\varphi < n/m < 2$, player A moves to $(m, n-m)$ since

$$\frac{m}{n-m} = \frac{1}{n/m-1} < \frac{1}{\varphi-1} = \varphi.$$

When $n/m > 2$ and $n \equiv r \pmod{m}$ for $0 \leq r < m$, there are two moves:

$$(n, m) \to (m, r) \text{ or } (n, m) \to (m+r, m).$$

If $r = 0$, player A wins. Otherwise, φ is between m/r and $(m+r)/m$. Player A moves to the position whose ratio lies strictly between 1 and φ.

Player B is left in position (a, b) where $1 < a/b < \varphi$. Player B must then move to (b, a') where $b/a' > \varphi$, from which the process is repeated. □

2×2 Matrices

A 2×2 matrix stores 4 pieces of information: $\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$.

To add two 2×2 matrices,

$$\mathbf{A} + \mathbf{B} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{bmatrix}.$$

To multiply a matrix $\mathbf{A}$ by a vector $\vec{x}$,

$$\mathbf{A}\vec{x} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 \\ a_{21}x_1 + a_{22}x_2 \end{bmatrix}.$$

To multiply two 2×2 matrices,

$$\mathbf{AB} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{bmatrix}.$$

Bézout's Identity Example

Example. Find integers m and n such that $107m + 44n = 1$.

Solution. The first method uses the Euclidean algorithm in reverse:

$$\begin{array}{rcl} 107 = 44 \cdot 2 + 19 & & 1 = 7 \cdot \underline{107} - 17 \cdot \underline{44} \quad \uparrow \\ 44 = 19 \cdot 2 + 6 & & 1 = -3 \cdot \underline{44} + 7 \cdot \underline{19} \quad \uparrow \\ 19 = 6 \cdot 3 + 1 & \Longrightarrow & 1 = \underline{19} - 3 \cdot \underline{6} \quad \uparrow \end{array}$$

Another method rewrites the first equation as $\begin{bmatrix} 107 \\ 44 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 44 \\ 19 \end{bmatrix}$.

Continuing in this manner by looking at the quotients,

$$\begin{bmatrix} 107 \\ 44 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 6 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Let $\mathbf{M}$ represent the product of all the quotient matrices. We compute

$$\mathbf{M} = \begin{bmatrix} 107 & 17 \\ 44 & 7 \end{bmatrix}.$$

Inverses and Determinants

The inverse of a 2×2 matrix $\mathbf{A}$ is a matrix A^{-1} such that

$$\mathbf{A}\mathbf{A}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

We can compute an explicit formula for the inverse:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

The determinant of a 2×2 matrix is defined by

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Determinants are distributive, therefore $\det \mathbf{AB} = \det \mathbf{A} \det \mathbf{B}$.

Matrix Form of Euclidean Algorithm

Theorem. The gcd of two integers a and b can be computed by:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ &\cdots \\ r_{n-2} &= q_n r_{n-1} + 0. \end{aligned}$$

We rewrite this as a product of quotient matrices and a remainder vector:

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} b \\ r_0 \end{bmatrix} = \begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} r_0 \\ r_1 \end{bmatrix} = \cdots = \prod_{i=0}^{n} \begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} r_{n-1} \\ 0 \end{bmatrix}.$$

Let $\mathbf{M} = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}$ represent the product of all the quotient matrices.

Matrix Form of Bézout's Identity

If $\mathbf{M} = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} = \prod_{i=0}^{n} \begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix}$, then the Euclidean algorithm is

$$\begin{bmatrix} a \\ b \end{bmatrix} = \mathbf{M} \begin{bmatrix} r_{n-1} \\ 0 \end{bmatrix} = \mathbf{M} \begin{bmatrix} g \\ 0 \end{bmatrix}.$$

To express g as a linear combination of a and b, we must compute $\mathbf{M}^{-1}$. We see $\det \mathbf{M} = (-1)^{n+1}$, since it equals the product of the determinants of the quotient matrices, each of which is negative one. By the inverse formula,

$$\begin{bmatrix} g \\ 0 \end{bmatrix} = \mathbf{M}^{-1} \begin{bmatrix} a \\ b \end{bmatrix} = (-1)^{n+1} \begin{bmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}.$$

The top equation is $g = (-1)^{n+1} (m_{22}a - m_{12}b)$, therefore integer solutions to $ax + by = g$ are $x = (-1)^{n+1} m_{22}$ and $y = (-1)^n m_{12}$.

Outline

Relevant Links

- Matt Parker: The Unbeatable Game from the 60s: Dr NIM
- Mathologer: NIM, or, always WIN with math
- Archimedes' Lab: Play Nim against your computer!
- CL Bouton: Nim, a Game with Complete Mathematical Theory.
- Steven Vajda: Mathematical Games and How to Play Them
- A Game Based on the Euclidean Algorithm and a Winning Strategy f