The Agoh-Giuga Conjecture

PROMYS Counselor Seminar

Joshua Im

July 22, 2025

1 Motivation

1.1 Fermat Pseudoprimes

We all know the Fermat's little theorem.

Theorem 1.1: Fermat's Little Theorem

If p is a prime and $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Does the converse work? That is, if we have an integer a and positive integer n such that $a^{n-1} \equiv 1 \pmod{n}$, then is n prime? This test of checking if a given integer is a prime is called the Fermat test. This would be good algorithm to find prime numbers with calculating too much, if the converse was true.

Sadly, this does not hold. We have

$$2^{340} \equiv 1 \pmod{341},$$

but 341 is not prime as $341 = 11 \cdot 31$.

Definition 1.1: Fermat Pseudoprimes

A composite number n is a Fermat pseudoprime of base a if

$$a^{n-1} \equiv 1 \pmod{n}.$$

So 341 is a Fermat pseudoprime of base 2.

There are not many pseudoprimes (as the smallest one of base 2 is 341). Even if we know that $2^{340} \equiv 1 \pmod{n}$, changing the base will give a different number. For example, $3^{340} \equiv 56 \pmod{341}$. This clearly shows that 341 is not prime. So 341 passes the Fermat test of base 2, it cannot pass the Fermat test of base 3.

But what if...

1.2 Carmichael Numbers

Definition 1.2: Carmichael Numbers

A Carmichael number is a composite number n which satisfies

$$a^{n-1} \equiv 1 \pmod{n}$$

for all integers a such that $\gcd(a, n) = 1$.

Carmichael numbers will pass the Fermat tests of any bases!!

How do we find Carmichael numbers? There is a criterion for this.

Theorem 1.2: Korselt's Criterion

A positive compositie integer n is a Carmichael number if and only if n is squarefree, and for all prime divisors $p \mid n$, $p - 1 \mid n - 1$.

Proof. Assume n is a Carmichael number. If n is not squarefree, we have $n = p^k n'$ where $k \geq 2$ and $(p, n') = 1$. By Chinese remainder theorem, there is a unique $a \in \mathbb{Z}/n\mathbb{Z}$ such that $a \equiv 1 + p \pmod{p^k}$ and $a \equiv 1 \pmod{n'}$. Since n is a Carmichael number, $a^{n-1} \equiv 1 \pmod{n}$. We have $(1+p)^{n-1} \equiv 1 + (n-1)p \equiv 1 \pmod{p^2}$, so $1 - p \equiv 1 \pmod{p^2}$, a contradiction. Therefore $k = 1$.

Since n is squarefree, for any prime $p \mid n$, p and n/p are coprime. Since there is a primitive root modulo any prime, choose one primitive root $b \in \mathbb{Z}$. By the Chinese remainder theorem, there is a unique $a \in \mathbb{Z}/n\mathbb{Z}$ such that $a \equiv b \pmod{p}$ and $a \equiv 1 \pmod{n/p}$, so $\gcd(a, n) = 1$. Then $a^{n-1} \equiv \pmod{n}$, and $b^{n-1} \equiv 1 \pmod{p}$. Since b has order $p - 1$, $p - 1 \mid n - 1$.

Now assume n is squarefree and $(p-1) \mid (n-1)$ whenever $p \mid n$. If $a \in \mathbb{Z}$ satisfies $\gcd(a, n) = 1$ then for each prime p dividing n we have $\gcd(a, p) = 1$, so $a^{p-1} \equiv 1 \pmod{p}$. Since $p - 1 \mid n - 1$, we get $a^{n-1} \equiv \pmod{p}$. By the Chinese remainder theorem, the result follows. □

Corollary

All Carmichael numbers are odd.

Proof. Suppose there is a Carmichael number $n \geq 2$ that is even. Since n is squarefree, $n/2$ is odd, thus n should have an odd factor, call it p. Then $(p-1) \mid (n-1)$ gives even | odd, which is impossible. □

1.3 Wilson's Theorem

We will now look at Wilson's theorem, which can act as another criterion of finding primes.

Theorem 1.3: Wilson's Theorem

A positive integer n is prime if and only if

$$(n-1)! \equiv -1 \pmod{n}.$$

So if we want to know whether a given positive integer is prime, we can use Wilson's theorem. Wilson's theorem is a good criterion, using the multiplicative condition.

2 Giuga's Conjecture

2.1 Giuga's Conjecture

Wilson's theorem used the multiplicative condition, but we could also think whether there is a criterion using the additive condition. We introduce the Giuga's conjecture.

Conjecture 1: Giuga's Conjecture

The integer n is a prime number if and only if

$$\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}.$$

One side is easy to prove. If p is prime, then $k^{p-1} \equiv 1 \pmod{p}$ for all $k = 1, 2, \ldots, p-1$, so $\displaystyle\sum_{k=1}^{p-1} k^{p-1} \equiv -1 \pmod{p}$. However, the other side remains unsolved until this day.

It has been shown if there is a composite number n satisfies the formula above, then it is at least $13,800$ digits, which gives evidence that the statement is true.

2.2 Giuga Numbers

Definition 2.1: Giuga Numbers

A Giuga number is a composite number n such that for each of its distinct prime factors p_i, we have

$$p_i \mid \left(\frac{n}{p_i} - 1\right).$$

For example, 30 and 858 are Giuga numbers. The first few Giuga numbers are: 30, 858, 1722, 66198, 2214408306, 24423128562, 432749205173838, ...

We can observe that only squarefree integers could be Giuga numbers.

There are several equivalent formations of the definition of Giuga's number, and the most frequent one is the following theorem.

Theorem 2.1

A positive integer n is a Giuga number if and only if

$$\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} \in \mathbb{N}.$$

Proof. ($\Rightarrow$) Suppose n is a Giuga number. Then since n is squarefree, $\prod_{p|n} \frac{1}{p} = \frac{1}{n}$. Consider

$$n \sum_{p|n} \frac{1}{p} - 1.$$

For any prime p_i, divide the expression to

$$n \sum_{\substack{p|n \\ p \neq p_i}} \frac{1}{p} + \frac{n}{p_i} - 1.$$

Since n is squarefree, $p_i \mid \frac{n}{p}$ for $p_i \neq p$. Furtherfore, we have $p_i \mid \frac{n}{p_i} - 1$, so $p_i \mid n \sum_{p|n} \frac{1}{p} - 1$. Therefore $n \mid n \sum_{p|n} \frac{1}{p} - n$, and $\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} \in \mathbb{N}$.

($\Leftarrow$) This side of the proof is omitted. □

How does Giuga numbers related to Giuga's conjecture?

Lemma

Let p be a prime. Then for any positive integer n,

$$\sum_{k=1}^{p-1} k^{n-1} \equiv \begin{cases} -1 \pmod{p} & \text{if } (p-1) \mid (n-1) \\ 0 \pmod{p} & \text{it } (p-1) \nmid (n-1) \end{cases}.$$

Proof. Suppose $(p-1) \mid (n-1)$. Then for $k = 1, 2, \ldots, p-1$, we have $p \nmid k$, so $k^{p-1} \equiv 1 \pmod{p}$. This gives

$$\sum_{k=1}^{p-1} k^{n-1} \equiv 1 + 1 + \cdots + 1 = p - 1 \equiv -1 \pmod{p}.$$

Now, suppose $(p-1) \nmid (n-1)$. Take a primitive root g mod p. Then since

$\{1,2,\ldots,p-1\}=\{g,g^2,\ldots,g^{p-1}\}$, we have

$$\begin{aligned}\sum_{k=1}^{p-1}k^{n-1}&=g^{n-1}+g^{2n-2}+\cdots+g^{(p-1)(n-1)}\\&=g^{n-1}\cdot\frac{g^{(p-1)(n-1)}-1}{g^{n-1}-1}\\&\equiv 0\pmod p\end{aligned}$$

since $g^{p-1}\equiv 1\pmod p$. □

Theorem 2.2

A composite number satisfies the Giuga's condition if and only if it is both a Carmichael number and a Giuga number.

Proof. ($\Rightarrow$) Suppose a composite number satisfies the Giuga's condition. Take a prime p, and let $n=pq$ (note that q is not necessarily coprime with p, that is n may not be squarefree). Then we have

$$\begin{aligned}\sum_{k=1}^{n-1}k^{n-1}&=\sum_{\substack{1\le k\le n-1\\p\nmid n}}k^{n-1}+\sum_{\substack{1\le k\le n-1\\p\mid n}}k^{n-1}\\&\equiv q\sum_{\substack{1\le k\le n-1\\p\nmid n}}k^{n-1}\pmod p\\&=\begin{cases}-q\pmod p & \text{if }(p-1)\mid(n-1)\\0\pmod p & \text{it }(p-1)\nmid(n-1)\end{cases}.\end{aligned}$$

This gives that $-q\equiv -1\pmod p$ and $(p-1)\mid(n-1)$. Since $q\equiv 1\pmod p$ and $q=n/p$, we have $p\mid\frac{n}{p}-1$, which is the Giuga's condition.

Finally, suppose n is not squarefree, so we have some prime $p_i\mid n$ such that $p_i^2\mid n$. Then since n is Giuga, $p_i\mid\frac{n}{p_i}-1$. But $p_i\mid\frac{n}{p_i}$, which is a contradiction to that p_i is prime. Therefore, since n is squarefree and $(p-1)\mid(n-1)$ for every prime $p\mid n$, n is Carmichael.

($\Leftarrow$) Suppose a composite number is both Carmichael and Giuga. Then we can write $n=p_1p_2\cdots p_k$ (since all Carmichael numbers are squarefree). We claim that

$$\sum_{k=1}^{n-1}k^{n-1}\equiv -1\pmod{p_i}$$

for all primes $p_i \mid n$. Since n is Carmichael, $p_i - 1 \mid n - 1$. We have

$$\begin{aligned}
\sum_{k=1}^{n-1} k^{n-1} &= \sum_{\substack{1\le k\le n-1 \\ p_i \nmid n}} k^{n-1} + \sum_{\substack{1\le k\le n-1 \\ p_i \mid n}} k^{n-1} \\
&\equiv 1 \cdot \left(n - \frac{n}{p_i}\right) \pmod{p_i} \\
&\equiv \left(n - \frac{n}{p_i}\right) + \left(\frac{n}{p_i} - 1\right) \pmod{p_i} \\
&\equiv -1 \pmod{p_i}.
\end{aligned}$$

The result follows by Chinese remainder theorem. □

2.3 Arithmetic Derivatives

Theorem 2.3: Arithmetic Derivative

The arithmetic derivative is defined as the function $D : \mathbb{Z} \to \mathbb{Z}$ by

- $D(1) = D(0) = 0$
- $D(p) = 1$ for primes p
- $D(ab) = aD(b) + bD(a)$ for any $a, b \in \mathbb{N}$ (Leibniz rule)
- $D(-n) = D(n)$.

We also use the notation $D(n) = n'$.

Lemma : Power Rule

If p is a prime, then $D(p^k) = kp^{k-1}$.

Proof. We use Induction. If $k = 1$, then $D(p^1) = 1 \cdot p^0 = 1$. Suppose $D(p^i) = ip^{i-1}$. Then $D(p^{i+1}) = pD(p^i) + p^i D(p) = p \cdot ip^{i-1} + p^i = (i+1)p^i$, so we're done. □

Theorem 2.4

If $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then

$$n' = n \sum_{i=1}^{r} \frac{e_i}{p_i}.$$

Proof. We use induction on distinct prime factors of n. If $n = p_1^{e_1}$, then $n' = n \cdot \dfrac{e_1}{p_1} = e_1 p^{e_1 - 1}$. Suppose $n = p_1^{e_1} p_2^{e_2} \cdots p_j^{e_j}$, and $n' = n \sum_{i=1}^{j} \dfrac{e_i}{p_i}$. Then if $n =$

$p_1^{e_1}p_2^{e_2}\cdots p_j^{e_j}p_{j+1}^{e^{j+1}}$, we have

$$\begin{aligned} n' &= p_{j+1}^{e_{j+1}}D(p_1^{e_1}p_2^{e_2}\cdots p_j^{e_j}) + p_1^{e_1}p_2^{e_2}\cdots p_j^{e_j}D(p_{j+1}^{e_{j+1}}) \\ &= p_{j+1}^{e_{j+1}}\cdot p_1^{e_1}p_2^{e_2}\cdots p_j^{e_j}\sum_{i=1}^{j}\frac{e_i}{p_i} + p_1^{e_1}p_2^{e_2}\cdots p_j^{e_j}\cdot e_{j+1}p^{e_{j+1}-1} \\ &= p_1^{e_1}p_2^{e_2}\cdots p_j^{e_j}p_{j+1}^{e^{j+1}}\left(\sum_{i=1}^{j}\frac{e_i}{p_i} + \frac{e_{j+1}}{p_{j+1}}\right) \\ &= p_1^{e_1}p_2^{e_2}\cdots p_j^{e_j}p_{j+1}^{e^{j+1}}\sum_{i=1}^{j+1}\frac{e_i}{p_i}. \end{aligned}$$

□

Corollary

If $n = p_1p_2\cdots p_r$ is a squarefree number, then

$$n' = n\sum_{i=1}^{r}\frac{1}{p_i}.$$

2.4 Arithmetic Derivatives and Giuga Numbers

Theorem 2.5

A positive integer is a Giuga number if and only if it satisfies $n' = an + 1$ for some $a \in \mathbb{N}$.

Proof. Suppose n is a Giuga number, then let $\displaystyle\sum_{p|n}\frac{1}{p} - \prod_{p|n}\frac{1}{p} = a \in \mathbb{N}$. Since n is squarefree, we have

$$\begin{aligned} n\left(\sum_{p|n}\frac{1}{p} - \prod_{p|n}\frac{1}{p}\right) &= n\sum_{p|n}\frac{1}{p} - 1 \\ &= n' - 1 \\ &= an. \end{aligned}$$

Conversely, suppose n satisfies $n' = an + 1$ for some $a \in \mathbb{N}$. Let $n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$. Then we have

$$n' = n\sum_{i=1}^{r}\frac{e_i}{p_i} = an + 1.$$

Now we prove that n is squarefree. Suppose there is a prime $p \mid n$ such that $p^2 \mid n$.

Then $p \mid n'$, but $p \nmid an+1$. Therefore all e_is are 1, and we have

$$n' = n\sum_{i=1}^{r}\frac{1}{p_i} = an+1.$$

Rearranging gives

$$n\sum_{i=1}^{r}\frac{1}{p_i} - 1 = an$$

$$\sum_{i=1}^{r}\frac{1}{p_i} - \frac{1}{n} = a$$

$$\sum_{p|n}\frac{1}{p} - \prod_{p|n}\frac{1}{p} = a$$

with $a \in \mathbb{N}$. □

Why do these matter? The arithmetic derivative turns additive properties of numbers into equations involving a derivative-like operation. The arithmetic derivative have some analogue to arithmetical functions. For example, $D(n) = 0$ only for $n = 0$ and $n = 1$, and $D(n) = n$ if and only if n is perfect. Arithmetic derivatives also connects to differential algebra. Even if its rephrasing, this gives new ways to approach the problem.

3 Agoh's Conjecture

3.1 Bernoulli Numbers and Bernoulli Polynomials

Definition 3.1: Bernoulli Numbers

The Bernoulli numbers B_k, where k is a nonnegative integer, is defined by the generating function

$$\frac{x}{e^x - 1} = \sum_{k\geq 0} B_k \frac{x^k}{k!}.$$

Some numerical values are:

- $B_0 = 1$
- $B_1 = -1/2$
- $B_2 = 1/6$
- $B_3 = 0$

- $B_4 = -1/30$
- $B_5 = 0$
- $B_6 = -1/42$

Definition 3.2: Bernoulli Polynomials

The Bernoulli polynomials $B_k(x)$, where k is a nonnegative integer, is defined by the generating function

$$\frac{te^{xt}}{e^t - 1} = \sum_{k\geq 0} B_k(x)\frac{t^k}{k!}.$$

The first Bernoulli polynomials are:

- $B_0(x) = 1$
- $B_1(x) = x - \frac{1}{2}$
- $B_2(x) = x^2 - x + \frac{1}{6}$
- $B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x.$

Two important properties will be needed later.

- Letting $x = 0$ on the generating function of Bernoulli polynomials, we get $B_n(0) = B_n$.
- Taking $\dfrac{\partial}{\partial x}$ on the generating function of Bernoulli polynomials, we get $B_n'(x) = nB_{n-1}(x)$.

3.2 Agoh's Conjecture

Conjecture 2: Agoh's Conjecture

The integer p is a prime number if and only if

$$pB_{p-1} \equiv -1 \pmod{p}.$$

where B_n is the nth Bernoulli number.

This conjecture is actually equivalent to the Giuga's conjecture, so they are called in Agoh-Giuga conjecture. In later sections, we will prove that the two statements are equal.

3.3 Stirling Numbers of the Second Kind

Define $S_n(m) = \sum_{k=1}^{m} k^n$.

Definition 3.3: Stirling Numbers of the Second Kind

The Stirling numbers of the second kind, denoted $S(n,k)$ or $\left\{ n \atop k \right\}$, is the number of ways to partition a set of n objects into k nonempty subsets.

Definition 3.4: Falling Factorials

If x is a real number, for a positive integer n, define the falling factorial $(x)_n = x(x-1)\cdots(x-n+1)$.

Theorem 3.1

$$x^n = \sum_{k=0}^{n} \left\{ n \atop k \right\} (x)_k.$$

Proof. Proof omitted. □

Definition 3.5: Generalized Binomial Coefficients

If x is a real number, then for a positive integer k, the generalized binomial coeffcient $\binom{x}{k}$ is defined as

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!} = \frac{(x)_k}{k!}.$$

Lemma

We have the following forward difference relation: $B_n(x+1) - B_n(x) = nx^{n-1}$.

Proof. Since $\dfrac{te^{tx}}{e^t-1} = \displaystyle\sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!}$, substituting $x+1$ gives

$$\frac{te^{t(x+1)}}{e^t-1} = \sum_{n=0}^{\infty} B_n(x+1)\frac{t^n}{n!}.$$

Subtracting the first expression from the second expression gives

$$\frac{te^{t(x+1)}}{e^t-1} - \frac{te^{tx}}{e^t-1} = \sum_{n=0}^{\infty} \left(B_n(x+1) - B_n(x)\right)\frac{t^n}{n!}$$

$$te^{tx}\frac{e^t-1}{e^t-1} = \sum_{n=0}^{\infty} \left(B_n(x+1) - B_n(x)\right)\frac{t^n}{n!}.$$

So the left-hand side is te^{tx}, which has Taylor series

$$te^{tx} = \sum_{n=1}^{\infty} \frac{x^{n-1}t^n}{(n-1)!} = \sum_{n=1}^{\infty} nx^{n-1} \cdot \frac{t^n}{n!}.$$

Therefore, we should have $B_0(x+1) - B_0(x) = 0$, and $B_n(x+1) - B_n(x) = nx^{n-1}$ for $n \geq 1$, which gives $B_n(x+1) - B_n(x) = nx^{n-1}$ for $n \geq 0$. □

Theorem 3.2

Let x be a real number and n be a positive integer. Then

$$S_n(x) = \sum_{k=1}^{n} k! \left\{ {n \atop k} \right\} \binom{x}{k+1} \quad \text{and} \quad B_n = \sum_{k=1}^{n} k! \left\{ {n \atop k} \right\} \frac{(-1)^k}{k+1}.$$

Proof. If m is a positive integer, then

$$\begin{aligned} S_n(m) &= \sum_{i=1}^{m-1} i^n \\ &= \sum_{i=1}^{m-1}\sum_{k=0}^{n} \left\{ {n \atop k} \right\} (i)_n \\ &= \sum_{i=1}^{m-1}\sum_{k=0}^{n} k! \left\{ {n \atop k} \right\} \binom{i}{k} \\ &= \sum_{k=1}^{n} k! \left\{ {n \atop k} \right\} \sum_{i=1}^{m-1} \binom{i}{k} \\ &= \sum_{k=1}^{n} k! \left\{ {n \atop k} \right\} \binom{m}{k+1}. \end{aligned}$$

So $S_n(m)$ is a polynomial of degree $n+1$, so $S_n(x) = \sum_{k=1}^{n} k! \left\{ {n \atop k} \right\} \binom{x}{k+1}$. Since

$S_n(0) = 0$ and $\binom{-1}{k} = (-1)^k$, we have

$$\begin{aligned} S_n'(0) &= \lim_{x\to 0} \frac{S_n(x)}{x} \\ &= \lim_{x\to 0} \sum_{k=1}^{n} k! \left\{ {n \atop k} \right\} \binom{m}{k+1} \binom{x-1}{k} \\ &= \sum_{k=1}^{n} k! \left\{ {n \atop k} \right\} \binom{m}{k+1} \frac{(-1)^k}{k+1}. \end{aligned}$$

Also,

$$S_n'(0) = \frac{d}{dx}\left(\frac{B_{n+1}(x) - B_{n+1}}{n+1} \right)\Bigg|_{x=0} = B_n(0) = B_n,$$

thus $B_n = \displaystyle\sum_{k=1}^{n} k! \left\{ {n \atop k} \right\} \binom{m}{k+1} \frac{(-1)^k}{k+1}$. □

3.4 Equivalence of Two Conjectures

Lemma

We have $S_n(m) = \dfrac{B_{n+1}(m+1) - B_{n+1}(0)}{n+1}$.

Proof. We write the right-hand side as

$$\frac{B_{n+1}(m+1) - B_{n+1}(0)}{n+1} = \frac{\sum_{k=0}^{m} \left(B_{n+1}(k+1) - B_{n+1}(k) \right)}{n+1}$$

Then $B_{n+1}(k+1) - B_{n+1}(k) = (n+1)k^n$ by the previous lemma, we have

$$\begin{aligned} \frac{B_{n+1}(m+1) - B_{n+1}(0)}{n+1} &= \frac{\sum_{k=0}^{m} (n+1)k^n}{n+1} \\ &= \sum_{k=0}^{m} k^n \\ &= S_n(m). \end{aligned}$$ □

Theorem 3.3

$S_{n-1}(n-1) \equiv nB_{n-1} \pmod{n}$.

Proof. By the lemma above, we have

$$\begin{aligned} S_{n-1}(n-1) &= \frac{B_n(n)-B_n(0)}{n} \\ &= \frac{\sum_{k=0}^{n}\binom{n}{k}B_k n^{n-k} - B_n}{n} \\ &= \frac{\sum_{k=0}^{n-1}\binom{n}{k}B_k n^{n-k} + B_n - B_n}{n} \\ &= \frac{\sum_{k=0}^{n-2}\binom{n}{k}B_k n^{n-k}}{n} + nB_{n-1}. \end{aligned}$$

We now need to show that $n^2 \mid \sum_{k=0}^{n-2}\binom{n}{k}B_k n^{n-k}$ for all $k = 0, 1, \ldots, n-2$, which we assume for this handout. The proof uses Stirling numbers of the second kind and theorem 3.2. Therefore, we have $S_{n-1}(n-1) \equiv nB_{n-1} \pmod{n}$. □

4 Related Open Problems

We state some related conjectures that has not been proved.

Conjecture 3: Odd Giuga Numbers

There are no odd Giuga numbers.

This immediately proves Giuga's conjecture, since any counterexample to the Giuga's conjecture should be Carmichael, which is odd.

Conjecture 4: Lava's Conjecture

A positive integer n is a Giuga number if and only if it satisfies

$$n' = n + 1.$$

Or, if n is a Giuga number if and only if

$$\sum_{p|n}\frac{1}{p} - \prod_{p|n}\frac{1}{p} = 1.$$

So even if we have $n' = an + 1$ for some $a \in \mathbb{N}$, the conjecture says that if n is Giuga, then a is always 1. The first few Giuga numbers are: 30, 858, 1722, 66198, 2214408306, 24423128562, 432749205173838, ..., and the corresponding a were all 1.