Adventures in arithmetic

Paul Pollack

University of Illinois at Urbana-Champaign

April 11, 2011

PART I: AN ALGEBRAIC AFFAIR

Twin primes

Recall: A pair of prime numbers $\{p, p+2\}$ is called a *twin prime pair*.

Twin primes

Recall: A pair of prime numbers $\{p, p+2\}$ is called a *twin prime pair*.

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, . . .

Twin primes

Recall: A pair of prime numbers $\{p, p+2\}$ is called a *twin prime pair*.

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, . . .

Twin prime pairs: {3, 5}, {5, 7}, {11, 13}, {17, 19}, {29, 31}, {41, 43}, {59, 61}, {71, 73}, . . .

Twin primes

Recall: A pair of prime numbers $\{p, p+2\}$ is called a *twin prime pair*.

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, ...

Twin prime pairs: $\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}$, $\{17, 19\}$, $\{29, 31\}$, $\{41, 43\}$, $\{59, 61\}$, $\{71, 73\}$, ...

Conjecture

There are infinitely many twin prime pairs. In other words, letting

$$\pi_2(x) := \#\{p \leq x : p, p+2 \textit{ both prime}\},$$

we have $\pi_2(x) \to \infty$ *as* $x \to \infty$.

Polynomials

Let $\mathbb{F}_q$ be a finite field. Call a pair of polynomials $f, f+1 \in \mathbb{F}_q[T]$ a *twin prime pair* if both f and $f+1$ are irreducible.

Example

For any $\mathbb{F}_q$, the polynomials T and $T+1$ are a twin prime pair. Over $\mathbb{F}_{11}$, take (say) $f := T^5 + T^4 + T^3 + 3$.

Conjecture

If $\mathbb{F}_q$ is a finite field and $q > 2$, then there are infinitely many twin prime pairs.

Polynomials

Let $\mathbb{F}_q$ be a finite field. Call a pair of polynomials $f, f+1 \in \mathbb{F}_q[T]$ a *twin prime pair* if both f and $f+1$ are irreducible.

Example

For any $\mathbb{F}_q$, the polynomials T and $T+1$ are a twin prime pair. Over $\mathbb{F}_{11}$, take (say) $f := T^5 + T^4 + T^3 + 3$.

Conjecture

If $\mathbb{F}_q$ is a finite field and $q > 2$, then there are infinitely many twin prime pairs.

Theorem (C. Hall)

The conjecture holds for all $q > 3$.

Theorem (P.)

The conjecture holds.

Polynomials, ctd.

Theorem (Capelli)

Let F be a field. Consider the binomial $f(T) := T^n - \alpha$, where $\alpha \in F$. Then f is irreducible over F unless one of the following two cases occurs:

- *α is an ℓth power for some prime ℓ dividing n,*
- *$4 \mid n$ and $\alpha = -4\beta^4$ for some $\beta \in F$.*

Remark

If either of these two cases occurs, then f is reducible. Notice that we have the identity

$$X^4 + 4Y^4 = (X^2 + 2Y^2)^2 - (2XY)^2.$$

Theorem

The conjecture is true for $F = \mathbb{F}_7$.

Theorem

The conjecture is true for $F = \mathbb{F}_7$.

Proof.

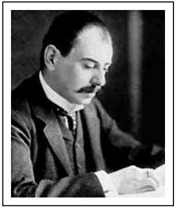
Let $k \geq 0$, and consider the binomial $T^{3^k} - 2 \in \mathbb{F}_7[T]$. The only third powers in $\mathbb{F}_7$ are $0, 1, -1$ (by explicit computation), and so 2 and 3 are not cubes. Also, $4 \nmid 3^k$. So

$$T^{3^k} - 2 \text{ is irreducible.}$$

Similarly,

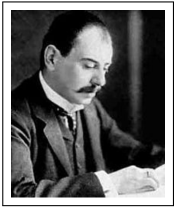
$$T^{3^k} - 3 \text{ is irreducible.}$$

So for every k, we have a pair of irreducibles of degree 3^k that differ by 1.



Conjecture (Goldbach–Euler, Landau)

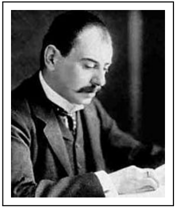
There are infinitely many primes that are one more than a perfect square; in other words, the polynomial $n^2 + 1$ *represents infinitely many primes as* n *runs over the natural numbers.*



Conjecture (Goldbach–Euler, Landau)

There are infinitely many primes that are one more than a perfect square; in other words, the polynomial $n^2 + 1$ *represents infinitely many primes as* n *runs over the natural numbers.*

Question: Are there infinitely many irreducible polynomials of the form $f^2 + 1$, where f is in $\mathbb{F}_q[T]$?



Conjecture (Goldbach–Euler, Landau)

There are infinitely many primes that are one more than a perfect square; in other words, the polynomial $n^2 + 1$ represents infinitely many primes as n runs over the natural numbers.

Question: Are there infinitely many irreducible polynomials of the form $f^2 + 1$, where f is in $\mathbb{F}_q[T]$?

Theorem (P.)

Suppose -1 is not a square in $\mathbb{F}_q$. Then there are infinitely many polynomials f for which $f^2 + 1$ is irreducible over $\mathbb{F}_q$.

Fix a square root i of -1 from the extension $\mathbb{F}_{q^2}$. We have

$$h(T)^2 + 1 \text{ irreducible over } \mathbb{F}_q \iff h(T) - i \text{ irreducible over } \mathbb{F}_{q^2}.$$

Try for $h(T)$ a binomial – say $h(T) = T^{\ell^k} - \beta$, with ℓ a fixed prime. By Capelli, it suffices to find $\beta \in \mathbb{F}_q$ so that $\beta + i$ is a non-ℓth power in $\mathbb{F}_{q^2}$.

Fix a square root i of -1 from the extension $\mathbb{F}_{q^2}$. We have

$$h(T)^2 + 1 \text{ irreducible over } \mathbb{F}_q \iff h(T) - i \text{ irreducible over } \mathbb{F}_{q^2}.$$

Try for $h(T)$ a binomial – say $h(T) = T^{\ell^k} - \beta$, with ℓ a fixed prime. By Capelli, it suffices to find $\beta \in \mathbb{F}_q$ so that $\beta + i$ is a non-ℓth power in $\mathbb{F}_{q^2}$.

New (old) ideas:

- Detect non-ℓth powers using characters!
- Use sharp bounds on character sums coming from Weil's Riemann Hypothesis for curves.

Choose any prime ℓ dividing $q^2 - 1$, and let χ be an ℓth power-residue character on $\mathbb{F}_{q^2}$. If there is no such β, then

$$\sum_{\beta \in \mathbb{F}_q} \chi(\beta + i) = q.$$

But Weil's Riemann Hypothesis gives a bound for this incomplete character sum of $\sqrt{q}$, a contradiction.

A more general conjecture

What about simultaneous prime values of higher degree polynomials (cf. Schinzel's Hypothesis H)?

Conjecture

Suppose $f_1, \ldots, f_r$ are irreducible polynomials in $\mathbb{F}_q[T]$ and that there is no irreducible P in $\mathbb{F}_q[T]$ for which

$$P(T) \text{ always divides } f_1(h(T)) \cdots f_r(h(T)).$$

Then $f_1(h(T)), \ldots, f_r(h(T))$ are simultaneously irreducible for infinitely many polynomials $h(T) \in \mathbb{F}_q[T]$.

A more general conjecture

What about simultaneous prime values of higher degree polynomials (cf. Schinzel's Hypothesis H)?

Conjecture

Suppose $f_1, \ldots, f_r$ are irreducible polynomials in $\mathbb{F}_q[T]$ and that there is no irreducible P in $\mathbb{F}_q[T]$ for which

$$P(T) \text{ always divides } f_1(h(T)) \cdots f_r(h(T)).$$

Then $f_1(h(T)), \ldots, f_r(h(T))$ are simultaneously irreducible for infinitely many polynomials $h(T) \in \mathbb{F}_q[T]$.

Our methods (Capelli + Weil) establish this when q is large vs.

$$D := \sum_{i=1}^{r} \deg f_i.$$

Let's get quantitative

Our proof of the twin prime conjecture for $\mathbb{F}_q$ gives very weak *quantitative results* on the number of twin primes.

Let's get quantitative

Our proof of the twin prime conjecture for $\mathbb{F}_q$ gives very weak *quantitative results* on the number of twin primes.

What do we expect?

Let $\pi(x) := \#\{p \text{ prime} \leq x\}$.

Theorem (Prime number theorem)

As $x \to \infty$,

$$\pi(x) \sim \sum_{1<n\leq x} \frac{1}{\log n}.$$

In other words, the counting function behaves as one would expect if a natural number > 1 is prime with "probability" $\frac{1}{\log n}$.

We might guess that

$$\pi_2(x) \approx \sum_{1<n\leq x} \frac{1}{(\log n)^2}.$$

This is a little naive, but probably close to right:

We might guess that

$$\pi_2(x) \approx \sum_{1<n\le x} \frac{1}{(\log n)^2}.$$

This is a little naive, but probably close to right:

Conjecture (Twin prime conjecture, quantitative form)

$$\pi_2(x) \sim C \sum_{1<n\le x} \frac{1}{(\log n)^2},$$

where

$$C = 2\prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right).$$

Polynomials, revisited

Theorem (Gauss)

Over $\mathbb{F}_q$, the number $\pi(q; n)$ of monic irreducible polynomials of degree n is approximately q^n/n. In fact, $\pi(q; n) \sim q^n/n$, whenever $q^n \to \infty$.

There are q^n monic polynomials in total, so a degree n polynomial is irreducible with probability about $1/n$.

Polynomials, revisited

Theorem (Gauss)

Over $\mathbb{F}_q$, the number $\pi(q; n)$ of monic irreducible polynomials of degree n is approximately q^n/n. In fact, $\pi(q; n) \sim q^n/n$, whenever $q^n \to \infty$.

There are q^n monic polynomials in total, so a degree n polynomial is irreducible with probability about $1/n$.

Conjecture

Let $\pi_2(q; n)$ be the number of monic polynomials f of degree n over $\mathbb{F}_q$ for which f and $f + 1$ are both prime. Whenever $q^n \to \infty$,

$$\pi_2(q; n) \sim C(q)q^n/n^2,$$

where $C(q)$ is a normalizing factor.

Conjecture

Let $\pi_2(q;n)$ be the number of monic polynomials f of degree n over $\mathbb{F}_q$ for which f and $f+1$ are both prime. Whenever $q^n \to \infty$,

$$\pi_2(q;n) \sim C(q)q^n/n^2,$$

where $C(q)$ is a normalizing factor.

We can prove the correct asymptotic for $\pi_2(q;n)$ whenever q is significantly larger than n and $\gcd(q,2n)=1$. In this case, $C(q) \sim 1$.

Bary-Soroker (2010) has relaxed the restriction $\gcd(q,2n)=1$.

PART II: A COMBINATORIAL CONQUEST

A conjecture of Parkin and Shanks

Let $p(n)$ be the number of partitions of n, where a partition of n is a way of writing n as a sum of natural numbers, where the order of the summands does not matter. For example, $p(5) = 7$, corresponding to

$$5, \quad 4+1, \quad 3+2, \quad 3+1+1, \quad 2+1+1+1, \quad 2+2+1, \quad 1+1+1+1+1.$$

A conjecture of Parkin and Shanks

Let $p(n)$ be the number of partitions of n, where a partition of n is a way of writing n as a sum of natural numbers, where the order of the summands does not matter. For example, $p(5) = 7$, corresponding to

$$5, \quad 4+1, \quad 3+2, \quad 3+1+1, \quad 2+1+1+1, \quad 2+2+1, \quad 1+1+1+1+1.$$

We know quite a bit about the **asymptotic properties** of $p(n)$. For example, Hardy and Ramanujan proved that

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}} \quad (n \to \infty).$$

A conjecture of Parkin and Shanks

Let $p(n)$ be the number of partitions of n, where a partition of n is a way of writing n as a sum of natural numbers, where the order of the summands does not matter. For example, $p(5) = 7$, corresponding to

$$5, \quad 4+1, \quad 3+2, \quad 3+1+1, \quad 2+1+1+1, \quad 2+2+1, \quad 1+1+1+1+1.$$

We know quite a bit about the **asymptotic properties** of $p(n)$. For example, Hardy and Ramanujan proved that

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}} \quad (n \to \infty).$$

Arithmetic properties of $p(n)$ remain more mysterious, although we know much more than we used to.

Conjecture (Parkin–Shanks)

As $x \to \infty$, the values $p(n)$ become uniformly distributed modulo 2. In other words,

$$\#\{n \leq x : p(n) \text{ even}\} \sim \frac{1}{2}x \quad (x \to \infty).$$

Conjecture (Parkin–Shanks)

As $x \to \infty$, the values $p(n)$ become uniformly distributed modulo 2. In other words,

$$\#\{n \leq x : p(n) \text{ even}\} \sim \frac{1}{2}x \quad (x \to \infty).$$

This conjecture has been attacked by several authors (Kolberg, Subbarao, Nicolas–Rusza–Sarkőzy, Ahlgren, Ono).

Theorem

For large x, we have

$$\#\{n \leq x : p(n) \text{ even}\} \gg x^{1/2}(\log\log x)^{1/2}$$

and for every fixed K,

$$\#\{n \leq x : p(n) \text{ odd}\} \gg x^{1/2}(\log\log x)^{K} / \log x.$$

Multiplicative partitions

Let $f(n)$ be the number of factorizations of n, where a *factorization* of n is a way of writing n as a product of integers all larger than 1. We consider two factorizations the same if they differ only in the order of the factors. For example, $f(12) = 4$, corresponding to

$$2 \cdot 2 \cdot 3, \quad 2 \cdot 6, \quad 3 \cdot 4, \quad 12.$$

Multiplicative partitions

Let $f(n)$ be the number of factorizations of n, where a *factorization* of n is a way of writing n as a product of integers all larger than 1. We consider two factorizations the same if they differ only in the order of the factors. For example, $f(12) = 4$, corresponding to

$$2 \cdot 2 \cdot 3, \quad 2 \cdot 6, \quad 3 \cdot 4, \quad 12.$$

Again we have good asymptotic results.

Theorem (Oppenheim, Szekeres–Turán)

As $x \to \infty$,

$$\frac{1}{x} \sum_{n \le x} f(n) \sim \frac{e^{2\sqrt{\log x}}}{2\sqrt{\pi}(\log x)^{3/4}}.$$

Theorem (Canfield–Erdős–Pomerance)

Let

$$L(x) := x^{\log\log\log x/\log\log x}.$$

For each fixed $\epsilon > 0$*, there are infinitely many* n *with*

$$f(n) > n/L(n)^{1+\epsilon}.$$

However, there are only finitely many n *with*

$$f(n) > n/L(n).$$

Conjecture

As $x \to \infty$, $\#\{n \le x : f(n) \text{ even}\} \sim \frac{1}{2}x$.

Conjecture

As $x \to \infty$, $\#\{n \le x : f(n) \text{ even}\} \sim \frac{1}{2}x$.

Up to 10^4: 5401 odd values
Up to 10^5: 55407 odd values,
Up to 10^6: 563483 odd values.

Conjecture

As $x \to \infty$, $\#\{n \le x : f(n) \text{ even}\} \sim \frac{1}{2}x$.

Up to 10^4: 5401 odd values
Up to 10^5: 55407 odd values,
Up to 10^6: 563483 odd values.

Theorem (Zaharescu–Zaki)

For each $\epsilon > 0$ and all large x, we have

$$\#\{n \le x : f(n) \text{ even}\} > \left(\frac{1}{2\pi^2} - \epsilon\right) x$$

and

$$\#\{n \le x : f(n) \text{ odd}\} > \left(\frac{2}{\pi^2} - \epsilon\right) x.$$

Theorem (P.)

Fix an arithmetic progression $a \bmod m$*. Then the set of* n *for which*

$$f(n) \equiv a \pmod{m}$$

possesses an asymptotic density; that is,

$$\frac{1}{x}\#\{n \leq x : f(n) \equiv a \pmod{m}\}$$

tends to a limit as $x \to \infty$*. Moreover, there is an algorithm for computing the density to arbitrary precision.*

Theorem (P.)

Fix an arithmetic progression $a \bmod m$*. Then the set of* n *for which*

$$f(n) \equiv a \pmod{m}$$

possesses an asymptotic density; that is,

$$\frac{1}{x}\#\{n \leq x : f(n) \equiv a \pmod{m}\}$$

tends to a limit as $x \to \infty$*. Moreover, there is an algorithm for computing the density to arbitrary precision.*

Theorem (P.)

In the case when $m = 2$ *and* $a = 1$*, this density is between* 0.55 *and* 0.60*. So the values* $f(n)$ *are* **not** *uniformly distributed modulo* 2*.*

Revisiting the theorem of Zaharescu and Zaki

Define the kth Bell number B_k as the number of set partitions of a k-element set. Alternatively, the B_k are described by the exponential generating function

$$e^{e^x-1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}.$$

Theorem (Touchard, Radoux, Lunnon–Pleasants–Stephens)

The Bell numbers B_k are purely periodic to every modulus. The length of the period modulo p always divides $\frac{p^p-1}{p-1}$.

Now suppose that n is squarefree. The set of such n has a density, which is given by the product

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

For squarefree n with $k = \omega(n)$ prime factors,

$$f(n) = B_k \quad (k\text{th Bell number}).$$

Now suppose that n is squarefree. The set of such n has a density, which is given by the product

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

For squarefree n with $k = \omega(n)$ prime factors,

$$f(n) = B_k \quad (k\text{th Bell number}).$$

The Bell numbers start off

$$B_0 = 1, \quad B_1 = 1, \quad B_2 = 2, \quad \dots$$

and are purely periodic modulo 2 with period $\frac{2^2-1}{2-1} = 3$. Hence, we see that the parity of f is a function of k mod 3:

$$f(n) \equiv \begin{cases} 1 \pmod 2 & \text{if } k \equiv 0, 1 \pmod 3, \\ 0 \pmod 2 & \text{if } k \equiv 2 \pmod 3. \end{cases}$$

Lemma

The values $\omega(n)$ are uniformly distributed to every modulus M, as n ranges over the squarefree numbers. (In particular, for $M = 3$.)

Proof.

It's enough to show that for each Mth root of unity $\zeta \neq 1$, the sum $\sum_{\substack{n \le x \\ n \text{ squarefree}}} \zeta^{\omega(n)}$ possesses cancelation (is $o(x)$, as $x \to \infty$). This follows from known results on mean values of multiplicative functions.

Corollary

The density of squarefree numbers with $f(n)$ odd is $\frac{2}{3}\frac{6}{\pi^2} = \frac{4}{\pi^2}$ and the density of squarefree numbers with $f(n)$ even is $\frac{1}{3}\frac{6}{\pi^2} = \frac{2}{\pi^2}$.

The existence of the density

We want that $\mathcal{S} := \{n : f(n) \equiv a \pmod{m}\}$ has a density. Say that a number N is *squarefull* if p^2 divides N whenever p divides N.

For each n, write $n = AB$, with A squarefull, B squarefree, and $\gcd(A, B) = 1$. Here A is called the *squarefull part* of n. For each squarefull number A, put

$$\mathcal{S}_A := \{n : f(n) \equiv a \pmod{m}, \quad n \text{ has squarefull part } A\}.$$

Then $\mathcal{S} = \cup_A \mathcal{S}_A$.

The existence of the density

We want that $\mathcal{S} := \{n : f(n) \equiv a \pmod{m}\}$ has a density. Say that a number N is *squarefull* if p^2 divides N whenever p divides N.

For each n, write $n = AB$, with A squarefull, B squarefree, and $\gcd(A, B) = 1$. Here A is called the *squarefull part* of n. For each squarefull number A, put

$$\mathcal{S}_A := \{n : f(n) \equiv a \pmod{m}, \quad n \text{ has squarefull part } A\}.$$

Then $\mathcal{S} = \cup_A \mathcal{S}_A$.

Suffices to show each $d(\mathcal{S}_A)$ exists, and that $d(\mathcal{S}) = \sum_A d(\mathcal{S}_A)$.

The existence of the density

We want that $\mathcal{S} := \{n : f(n) \equiv a \pmod{m}\}$ has a density. Say that a number N is *squarefull* if p^2 divides N whenever p divides N.

For each n, write $n = AB$, with A squarefull, B squarefree, and $\gcd(A, B) = 1$. Here A is called the *squarefull part* of n. For each squarefull number A, put

$$\mathcal{S}_A := \{n : f(n) \equiv a \pmod{m}, \quad n \text{ has squarefull part } A\}.$$

Then $\mathcal{S} = \cup_A \mathcal{S}_A$.

Suffices to show each $d(\mathcal{S}_A)$ exists, and that $d(\mathcal{S}) = \sum_A d(\mathcal{S}_A)$. We will focus on showing each $d(\mathcal{S}_A)$ exists.

For n with squarefull part A, write

$$n = Ap_1 \cdots p_k$$

for some distinct primes $p_1, \ldots, p_k$ not dividing A.

For n with squarefull part A, write

$$n = Ap_1 \cdots p_k$$

for some distinct primes $p_1, \ldots, p_k$ not dividing A.
We will show that with A fixed, $f(n)$ modulo m is a periodic function of $\omega(n)$. By the $\omega(n)$ equidistribution lemma from before, the density of $\mathcal{S}_A$ exists.

For n with squarefull part A, write

$$n = Ap_1 \cdots p_k$$

for some distinct primes $p_1, \ldots, p_k$ not dividing A.
We will show that with A fixed, $f(n)$ modulo m is a periodic function of $\omega(n)$. By the $\omega(n)$ equidistribution lemma from before, the density of $\mathcal{S}_A$ exists.

Lemma (P.)

$$f(Ap_1 \cdots p_k) = \sum_{j=0}^{k} S(k,j) \sum_{d|A} f(d)\tau_j(A/d).$$

Here $S(k, j)$ is the number of set partitions of a k-element set into j parts (*Stirling number of the second kind*), and

$$\tau_j(n) = \sum_{d_1 \cdots d_j = n} 1.$$

Lemma (P.)

Fix an arithmetic progression, say $A \pmod{Q}$. Then

$$\sum_{\substack{0 \le j \le k \\ j \equiv A \pmod{Q}}} S(k, j)$$

is purely periodic modulo m as a function of k, for any modulus m.

Without the restriction on j, the sum is exactly B_k, the kth Bell number, and the lemma reduces to the theorem on periodicity of Bell numbers mentioned before.

Bell numbers can be defined by

$$\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = e^{e^x - 1}.$$

To prove the lemma, we need periodicity to any integer modulus of the generalized Bell numbers $B_n(\omega)$, defined by

$$\sum_{n=0}^{\infty} B_n(\omega) \frac{x^n}{n!} = e^{\omega(e^x - 1)},$$

where ω is a Qth root of unity.

Example

With $A = 1$, we have $1/3$ of the time $f(n)$ is even, and $2/3$ of the time, $f(n)$ is odd.

Example

With $A = 1$, we have $1/3$ of the time $f(n)$ is even, and $2/3$ of the time, $f(n)$ is odd. With $A = p^2$, one can check that $f(Ap_1 \cdots p_k)$ mod 2 cycles as

$$0, 0, 1, 0, 1, 0,$$

and so $f(n)$ is even $2/3$ of the time and odd $1/3$ of the time.

Example

With $A = 1$, we have $1/3$ of the time $f(n)$ is even, and $2/3$ of the time, $f(n)$ is odd. With $A = p^2$, one can check that $f(Ap_1 \cdots p_k)$ mod 2 cycles as

$$0, 0, 1, 0, 1, 0,$$

and so $f(n)$ is even $2/3$ of the time and odd $1/3$ of the time. With $A = p^3$, the cycle is

$$1, 1, 1, 0, 0, 1.$$

So $f(n)$ is even $1/3$ of the time and odd $2/3$ of the time.

Example

With $A = 1$, we have $1/3$ of the time $f(n)$ is even, and $2/3$ of the time, $f(n)$ is odd. With $A = p^2$, one can check that $f(Ap_1 \cdots p_k)$ mod 2 cycles as

$$0, 0, 1, 0, 1, 0,$$

and so $f(n)$ is even $2/3$ of the time and odd $1/3$ of the time. With $A = p^3$, the cycle is

$$1, 1, 1, 0, 0, 1.$$

So $f(n)$ is even $1/3$ of the time and odd $2/3$ of the time.

Collecting, we find the proportion of the time $f(n)$ is odd is at least

$$\frac{2}{3}\frac{6}{\pi^2} + \frac{1}{3}\left(\frac{6}{\pi^2}\sum_p \frac{1}{p(p+1)}\right) + \frac{2}{3}\left(\frac{6}{\pi^2}\sum_p \frac{1}{p^2(p+1)}\right) = 0.52165\ldots.$$

Thank you!