IRREDUCIBILITY TESTS IN $\mathbf{F}_p[T]$

KEITH CONRAD

1. Introduction

Let $\mathbf{F}_p = \mathbf{Z}/(p)$ be a field of prime order. We will discuss a few methods of checking if a polynomial $f(T) \in \mathbf{F}_p[T]$ is irreducible that are analogues of primality tests in $\mathbf{Z}$: trial division, the Fermat test, the Solovay–Strassen test, and the Miller–Rabin test. The proofs of these tests in $\mathbf{F}_p[T]$ are very similar to those in $\mathbf{Z}$, so they will all be left as exercises for the reader as an incentive to review the proofs in $\mathbf{Z}$.[1] It turns out that for the Miller–Rabin test in $\mathbf{F}_p[T]$ there is something new that can happen without an analogue in $\mathbf{Z}$, and for that result (the final theorem and corollary here) we give a proof.

Here is some terminology and notation related to the analogy between $\mathbf{Z}$ and $\mathbf{F}_p[T]$. The analogue in $\mathbf{F}_p[T]$ of positivity in $\mathbf{Z}$ is being *monic*: the leading coefficient is 1. For $n \in \mathbf{Z}^+$, the number of integers mod n is n, while for monic $f(T) \in \mathbf{F}_p[T]$ the number of polynomials mod $f(T)$ is $p^{\deg f}$. We call this the *norm* of f and write $\mathrm{N}(f) = p^{\deg f}$. Note in particular that $\mathrm{N}(f)$ is always a power of p and many monic polynomials can have the same norm, *e.g.*, in $\mathbf{F}_p[T]$ we have $\mathrm{N}(T + c) = p$ for every $c \in \mathbf{F}_q$. This is not like $\mathbf{Z}$, where there's just one positive integer per size. In $\mathbf{Z}$ a prime is usually denoted as p, and in $\mathbf{F}_p[T]$ an irreducible polynomial is usually denoted as $\pi = \pi(T)$. Two polynomials a and b in $\mathbf{F}_p[T]$ are called *relatively prime* if their only common factors are nonzero constants, in which case we write $(a, b) = 1$. If a and b have a nonconstant common factor then they are not relatively prime and we write $(a, b) \neq 1$.

2. Trial Division

In $\mathbf{Z}$, the most elementary method of proving an integer $n > 1$ is prime is trial division. If n has a nontrivial factorization $n = ab$ then $1 < a \leq \sqrt{n}$ or $1 < b \leq \sqrt{n}$. Therefore if n is not divisible by any integers (or just any prime numbers) that are greater than 1 and less than $\sqrt{n}$ then n is prime. The converse is obvious. There is a simple analogue of this in $\mathbf{F}_p[T]$ where $\sqrt{n}$ is replaced by $\frac{1}{2}\deg f$.

Theorem 2.1. *Let $f(T) \in \mathbf{F}_p[T]$ have degree $d \geq 2$. Then $f(T)$ is irreducible if and only if $f(T)$ is not divisible by any nonconstant monic polynomial of degree at most $d/2$.*

Proof. Exercise. □

Example 2.2. A polynomial $f(T)$ of degree 12 in $\mathbf{F}_p[T]$ is irreducible if and only if $f(T)$ is not divisible by any nonconstant monic polynomial of degree at most 6.

Testing a polynomial $f(T)$ for irreducibility by checking it is not divisible by any monic polynomial of degree from 1 to $\frac{1}{2}\deg f$ is called *trial division*, and it takes finitely many steps since there are only finitely many monic polynomials of any particular degree d (in fact, there are p^d such polynomials).

[1] Readers who know about general finite fields can extend the proofs to that case as an additional exercise.

3. The Fermat Test in $\mathbf{F}_p[T]$

An analogue of Fermat's little theorem in $\mathbf{Z}$ is true in $\mathbf{F}_p[T]$.

Theorem 3.1. *If π is irreducible in $\mathbf{F}_p[T]$ then $a^{\mathrm{N}(\pi)-1} \equiv 1 \bmod \pi$ for all $a \in \mathbf{F}_p[T]$ such that $(a, \pi) = 1$.*

Proof. Exercise. □

Here is the **Fermat test** for a nonconstant polynomial f in $\mathbf{F}_p[T]$: pick a random nonzero polynomial $a \in \mathbf{F}_p[T]$ with $\deg a < \deg f$ and check if $a^{\mathrm{N}(f)-1} \not\equiv 1 \bmod f$. If this happens even one time then f is reducible and we call such an a a *Femat witness* for f.

Example 3.2. Let $f(T) = T^5 + T^2 + 2$ in $\mathbf{F}_3[T]$. Here $\mathrm{N}(f) = 3^5 = 243$. We want to test $a^{242} \equiv 1 \bmod f$ when $\deg a < 5$. Already when $a = T$ we get a counterexample: $T^{242} \equiv T + 1 \not\equiv 1 \bmod f$, so f is reducible and T is a Fermat witness for f. Note $(T, f) = 1$.

An irreducible f has no Fermat witness while a reducible f has a Fermat witness, such as any nonconstant proper factor of f, but such a Fermat witness can be difficult to find by random searching. Often a Fermat witness is relatively prime to f, as in the previous example, in which case the next theorem tells us that there are many Fermat witnesses.

Theorem 3.3. *If $f \in \mathbf{F}_p[T]$ has a Fermat witness that is relatively prime to f then the proportion of Fermat witnesses for f,*

$$\frac{|\{a : \deg a < \deg f, a \text{ is a Fermat witness for } f\}|}{\mathrm{N}(f) - 1},$$

is greater than 50%.

Proof. Exercise. □

Unfortunately there are reducible polynomials f with no Fermat witness that is relatively prime to f. We call such f a *Carmichael polynomial*. That if, $f \in \mathbf{F}_p[T]$ is called Carmichael if f is reducible and $(a, f) = 1 \Longrightarrow a^{\mathrm{N}(f)-1} \equiv 1 \bmod f$ for all $a \in \mathbf{F}_p[T]$. Korselt's criterion in $\mathbf{Z}$ for Carmichael numbers has the following analogue for Carmichael polynomials.

Theorem 3.4. *A reducible polynomial $f \in \mathbf{F}_p[T]$ is Carmichael if and only if (i) f is squarefree[2] and (ii) for every monic irreducible π dividing f, also $(\mathrm{N}(\pi) - 1) \mid (\mathrm{N}(f) - 1)$.*

Proof. Exercise. □

Example 3.5. Every product of two or more different monic irreducibles of the same degree in $\mathbf{F}_p[T]$, such as $T(T + 1)$, is Carmichael.

This is an important type of example for at least two reasons. First of all, it shows that a Carmichael polynomial can have just two (monic) irreducible factors. In $\mathbf{Z}$ a Carmichael number has at least three prime factors. Second of all, since there are at least two monic irreducibles of each degree in $\mathbf{F}_p[T]$ except for degree 2 in $\mathbf{F}_2[T]$ (where $T^2 + T + 1$ is the only example), there are infinitely many Carmichael polynomials in each $\mathbf{F}_p[T]$. It is much harder to prove that there are infinitely many Carmichael numbers.

[2]For polynomials, "squarefree" means not being divisible by the square of a *nonconstant* polynomial. Being divisible by a constant square is not important, as every nonzero constant divides every polynomial.

Remark 3.6. The condition $(\mathrm{N}(\pi)-1)|(\mathrm{N}(f)-1)$ in Theorem 3.4 is equivalent to saying $\deg\pi \mid \deg f$. In particular, a product of two different monic irreducibles $\pi_1\pi_2$ is a Carmichael polynomial if and only if π_1 and π_2 have the same degree.

In $\mathbf{Z}$ every prime factor of a Carmichael number n is at most $\sqrt{n}$, and a composite $n \in \mathbf{Z}^+$ is Carmichael if and only if $a^n \equiv a \bmod n$ for all $a \in \mathbf{Z}$. Here are analogues in $\mathbf{F}_p[T]$.

Corollary 3.7. *In $\mathbf{F}_p[T]$ every irreducible factor of a Carmichael polynomial f has degree at most $\frac{1}{2}\deg f$, and a reducible $f \in \mathbf{F}_p[T]$ is Carmichael if and only if $a^{\mathrm{N}(f)} \equiv a \bmod f$ for all $a \in \mathbf{F}_p[T]$.*

Proof. Exercise. □

4. The Solovay–Strassen Test in $\mathbf{F}_p[T]$

Throughout this section p is odd.

For monic irreducible π and any $a \in \mathbf{F}_p[T]$, the *Legendre symbol* $(\frac{a}{\pi})$ is defined as follows:

$$\left(\frac{a}{\pi}\right) = \begin{cases} 1, & \text{if } a \equiv \square \bmod \pi \text{ and } a \not\equiv 0 \bmod \pi, \\ -1 & \text{if } a \not\equiv \square \bmod \pi, \\ 0, & \text{if } a \equiv 0 \bmod \pi. \end{cases}$$

Half the nonzero elements of $\mathbf{F}_p[T]/(\pi)$ are squares and half are nonsquares, so 1 and -1 are both values of $(\frac{a}{\pi})$ as a varies. If $p = 2$ then all elements of $\mathbf{F}_2[T]/(\pi)$ are squares; this is why we take p odd.

Here are five properties of the Legendre symbol in $\mathbf{F}_p[T]$. The second property is called Euler's congruence, the fourth is called the supplementary law of quadratic reciprocity, and the fifth is called the main law of quadratic reciprocity.

Theorem 4.1. *Let π be monic irreducible in $\mathbf{F}_p[T]$. For all a and b in $\mathbf{F}_p[T]$,*

1. *if $a \equiv b \bmod \pi$, then $(\frac{a}{\pi}) = (\frac{b}{\pi})$,*
2. *$a^{(\mathrm{N}(\pi)-1)/2} \equiv (\frac{a}{\pi}) \bmod \pi$,*
3. *$(\frac{ab}{\pi}) = (\frac{a}{\pi})(\frac{b}{\pi})$,*
4. *for all $c \in \mathbf{F}_p^\times$, $(\frac{c}{\pi}) = (\frac{c}{p})^{\deg\pi}$, where $(\frac{c}{p})$ is the Legendre symbol in $\mathbf{Z}$,*
5. *for distinct monic irreducibles π and $\widetilde{\pi}$ in $\mathbf{F}_p[T]$,*

$$\left(\frac{\widetilde{\pi}}{\pi}\right) = \begin{cases} \left(\dfrac{\pi}{\widetilde{\pi}}\right) & \text{if } \mathrm{N}(\pi) \text{ or } \mathrm{N}(\widetilde{\pi}) \equiv 1 \bmod 4, \\ -\left(\dfrac{\pi}{\widetilde{\pi}}\right) & \text{if } \mathrm{N}(\pi) \text{ and } \mathrm{N}(\widetilde{\pi}) \equiv 3 \bmod 4. \end{cases}$$

Proof. Exercise. The proof of the first three properties are very similar to the proofs of the analogous properties in $\mathbf{Z}$. For proofs of the last two properties see [2, Prop. 3.2, Theorem 3.3], taking $q = p$ and $d = 2$ there. □

Quadratic reciprocity in $\mathbf{F}_p[x]$ for odd p was first stated by Dedekind in 1857 [1]. He considered it sufficiently straightforward that he did not write down a proof. In the supplementary law, if $\deg\pi$ is even then $(\frac{c}{\pi}) = 1$ for all $c \in \mathbf{F}_p^\times$. In the main law, it is important that the irreducibles are monic; the formula is generally false without that. If $p \equiv 1 \bmod 4$ then $\mathrm{N}(f) = p^{\deg f} \equiv 1 \bmod 4$ for all f, so the main law has a simpler form in this case: $(\frac{\widetilde{\pi}}{\pi}) = (\frac{\pi}{\widetilde{\pi}})$.

The Jacobi symbol on $\mathbf{F}_p[T]$ is defined by extending the Legendre symbol multiplicatively in the denominator: for monic $f \in \mathbf{F}_p[T]$, let $f = \pi_1 \cdots \pi_r$ for monic irreducible π_i in $\mathbf{F}_p[T]$. Some of these irreducibles may be the same. For any $a \in \mathbf{F}_p[T]$ the *Jacobi symbol* $(\frac{a}{f})$ is

$$\left(\frac{a}{f}\right) = \left(\frac{a}{\pi_1}\right)\left(\frac{a}{\pi_2}\right)\cdots\left(\frac{a}{\pi_r}\right).$$

The value of $(\frac{a}{f})$ is ± 1 if $(a, f) = 1$ and it is 0 if $(a, f) \neq 1$.

All formulas we mentioned for the Legendre symbol in $\mathbf{F}_p[T]$ other than Euler's congruence are valid for the Jacobi symbol in $\mathbf{F}_p[T]$:

(1) If $a \equiv b \bmod f$, then $(\frac{a}{f}) = (\frac{b}{f})$.
(2) $(\frac{ab}{f}) = (\frac{a}{f})(\frac{b}{f})$.
(3) For all $c \in \mathbf{F}_p^\times$, $(\frac{c}{f}) = (\frac{c}{p})^{\deg f}$, where $(\frac{c}{p})$ on the right side is the Legendre symbol.
(4) For distinct monic f and g in $\mathbf{F}_p[T]$,

$$\left(\frac{g}{f}\right) = \begin{cases} \left(\dfrac{f}{g}\right) \text{ if } \mathrm{N}(f) \text{ or } \mathrm{N}(g) \equiv 1 \bmod 4, \\ -\left(\dfrac{f}{g}\right) \text{ if } \mathrm{N}(f) \text{ and } \mathrm{N}(g) \equiv 3 \bmod 4. \end{cases}$$

Proofs of these are left to the reader. The last two properties are called the supplementary law and main law of Jacobi reciprocity.

Euler's congruence breaks down for the Jacobi symbol in $\mathbf{Z}$, and similarly it breaks down in $\mathbf{F}_p[T]$:

Theorem 4.2. *Let $f(T)$ be monic reducible in $\mathbf{F}_p[T]$. There is an $a \in \mathbf{F}_p[T]$ such that $\deg a < \deg f$, $(a, f) = 1$, and $a^{(\mathrm{N}(f)-1)/2} \not\equiv (\frac{a}{f}) \bmod f$.*

Proof. Exercise. □

A nonzero $a \in \mathbf{F}_p[T]$ with $\deg a < \deg f$ satisfying either $(a, f) \neq 1$, or $(a, f) = 1$ and $a^{(\mathrm{N}(f)-1)/2} \not\equiv (\frac{a}{f}) \bmod f$, is called an *Euler witness* for f. We don't have to separately check if (a, f) is or is not 1, since the condition $(a, f) = 1$ is equivalent to $(\frac{a}{f})$ being ± 1 rather than 0.

Example 4.3. In $\mathbf{F}_7[T]$ let $f(T) = T^{10} + T^2 + 3$. The polynomial T is an Euler witness for f: since $\mathrm{N}(f) = 7^{10} \equiv 1 \bmod 4$ we have

$$\left(\frac{T}{f}\right) = \left(\frac{f}{T}\right) = \left(\frac{f(0)}{T}\right) = \left(\frac{3}{7}\right) = -1,$$

while a separate calculation shows $T^{(\mathrm{N}(f)-1)/2} \equiv 1 \bmod f$.

The irreducible factorization of f turns out to be

$$(T^5 + T^4 + 4T^3 + 6T^2 + 5T + 2)(T^5 + 6T^4 + 4T^3 + T^2 + 5T + 5),$$

so f is Carmichael (Theorem 3.4) and thus the Fermat test would not work for f unless we picked a polynomial with degree less than 10 that is not relatively prime to f. The proportion of such polynomials is $\approx .00011$, which is less than .1%.

Example 4.4. No $c \in \mathbf{F}_p^\times$ is an Euler witness for any f because $c^{(\mathrm{N}(f)-1)/2} = (\frac{c}{f})$ in $\mathbf{F}_p$ by the supplementary law of Jacobi reciprocity. This is analogous to ± 1 never being Euler witnesses in $\mathbf{Z}$. Therefore if we want to search for an Euler witness a for f we can take $\deg a \geq 1$ and we can also assume a is monic.

The proportion of Euler witnesses for a polynomial f is

$$\frac{|\{a : \deg a < \deg f, a \text{ is an Euler witness for } f\}|}{\mathrm{N}(f) - 1}.$$

Corollary 4.5. *Let f be nonconstant and monic in $\mathbf{F}_p[T]$.*

(1) *If f is irreducible, its proportion of Euler witnesses is 0%.*
(2) *If f is reducible, its proportion of Euler witnesses is greater than 50%.*

Proof. Exercise. □

Here is the **Solovay–Strassen test** to check a nonconstant f in $\mathbf{F}_p[T]$ for irreducibility:

(1) Randomly pick a nonzero polynomial a with $\deg a < \deg f$.
(2) Check if $(a, f) = 1$ and $a^{(\mathrm{N}(f)-1)/2} \equiv (\frac{a}{f}) \bmod f$, computing $(\frac{a}{f})$ by Jacobi reciprocity.
(3) If the answer is no then stop the test and declare (correctly) "f is reducible."
(4) If the answer is yes then repeat step 1.
(5) If the test runs for t trials without terminating then say "f is irreducible with probability at least $1 - 1/2^t$."

Example 4.6. In $\mathbf{F}_7[T]$ let $f(T) = T^9 + T^3 + 1$. To use the Solovay–Strassen test, pick random nonzero a with $1 \leq \deg a < 9$ (we can avoid constant a by Example 4.4) and test whether $(a, f) = 1$ and $a^{(\mathrm{N}(f)-1)/2} \equiv (\frac{a}{f}) \bmod f$. As soon as this fails we would know f is reducible. If $a(T) = T - c$ then the table below shows that after four trials we find an Euler witness, at $a = T - 3$. Thus $f(T)$ is reducible.

a	$a^{(\mathrm{N}(f)-1)/2} \bmod f$	$(\frac{a}{f})$
T	-1	-1
$T-1$	1	1
$T-2$	1	1
$T-3$	$T^8 + T^7 + 3T^5 + 4T^4 + 5T^2 + 4T + 2$	1

5. The Miller–Rabin Test in $\mathbf{F}_p[T]$

Throughout this section p is odd.

For any monic nonconstant f in $\mathbf{F}_p[T]$, $\mathrm{N}(f) = p^{\deg f}$ is odd and greater than 1. Write $\mathrm{N}(f) - 1 = 2^e k$ where $e \geq 1$ and k is odd. We call nonzero $a \in \mathbf{F}_p[T]$ with $\deg a < \deg f$ a *Miller–Rabin witness* for f if

$$a^k \not\equiv 1 \bmod f \text{ and } a^{2^i k} \not\equiv -1 \bmod f \text{ for all } i \in \{0, \ldots, e-1\}$$

and we say a is a *Miller–Rabin nonwitness* for f if

$$a^k \equiv 1 \bmod f \text{ or } a^{2^i k} \equiv -1 \bmod f \text{ for some } i \in \{0, \ldots, e-1\}.$$

The existence of a Miller–Rabin witness for f implies f is reducible.

Here is the **Miller–Rabin test** for deciding if monic nonconstant $f \in \mathbf{F}_p[T]$ is irreducible.

(1) Randomly pick a random nonzero a in $\mathbf{F}_p[T]$ with $\deg a < \deg f$.

(2) If a is a Miller–Rabin witness for f then stop the test and declare (correctly) "f is reducible."
(3) If a is not a Miller–Rabin witness for f then repeat step 1.
(4) If the test runs for t trials without terminating then say "n is prime with probability at least $1 - 1/2^t$."[3]

Example 5.1. In $\mathbf{F}_7[T]$ let $f(T) = T^{10} + T^2 + 3$, as in Example 4.3. Write $\mathrm{N}(f) - 1 = 7^{10} - 1 = 2^4 \cdot 17654703$, so $e = 4$ and $k = 17654703$. We will show T is a Miller–Rabin witness for f: $T^k \not\equiv 1 \bmod f$ and $T^{2^i k} \not\equiv -1 \bmod f$ for $i = 0, 1, 2$, and 3. With a computer,

$$T^k \equiv T^9 + 3T^7 + T^5 + 2T^3 + 2T \not\equiv 1 \bmod f \text{ and } T^{2k} \equiv 1 \bmod f.$$

Thus $T^{2^i k} \equiv 1 \bmod f$ for $i = 2$ and 3 as well.

Example 5.2. Let $f(T) = T^9 + T^3 + 1$ in $\mathbf{F}_7[T]$ as in Example 4.6. We will prove f is reducible by the Miller–Rabin test. Since $\mathrm{N}(f) - 1 = 7^9 - 1 = 2 \cdot (20176803)$, $e = 1$ and $k = 20176803$. Since $e = 1$, the Miller–Rabin test is picking random nonzero a with $\deg a < 9$ and checking if $a^k \not\equiv \pm 1 \bmod f$. As soon as we find such an a, f must be reducible. Since $a^k = a^{(\mathrm{N}(f)-1)/2}$, the Miller-Rabin test in this case amounts to checking for counterexamples to $a^{(\mathrm{N}(f)-1)/2} \equiv \pm 1 \bmod f$. Trying $a(T) = T - c$, we saw in Example 4.6 that a counterexample occurs when $a(T) = T - 3$.

Theorem 5.3. *For reducible $f \in \mathbf{F}_p[T]$, an Euler witness for f is a Miller–Rabin witness for f.*

Proof. Exercise. □

For monic reducible $f \in \mathbf{F}_p[T]$, the proportion of its Miller-Rabin witnesses is

$$\frac{|\{a : \deg a < \deg f, a \text{ is a Miller–Rabin witness for } f\}|}{\mathrm{N}(f) - 1}.$$

In $\mathbf{Z}$ the proportion of Miller–Rabin witnesses for any odd composite integer n is at least 75% of the numbers mod n (with equality only at $n = 9$). In that proof it is important in one step that an integer with only two prime factors is not a Carmichael number. But in $\mathbf{F}_p[T]$ a product of two different monic irreducibles *can* be a Carmichael polynomial, namely when the two irreducibles have the same degree; see Remark 3.6. If we stay away from such polynomials then the lower bound of 75% for the proportion of Miller–Rabin witnesses in $\mathbf{Z}$ remains true in $\mathbf{F}_p[T]$.

Theorem 5.4. *If $f \in \mathbf{F}_p[T]$ is monic reducible and f is not $\pi_1\pi_2$ where π_1 and π_2 are different monic irreducibles of the same degree then the proportion of Miller–Rabin witnesses for f is at least 75%, with equality if and only if $\mathrm{N}(f) = 9$, or equivalently $p = 3$ and $f(T) = (T + c)^2$ where $c \in \mathbf{F}_3$.*

Proof. Exercise. □

If $f = \pi_1\pi_2$ for different monic irreducibles π_1 and π_2 with $\deg \pi_1 = \deg \pi_2$, can its proportion of Miller–Rabin witnesses be less than 75%?

Example 5.5. In $\mathbf{F}_7[T]$ let $f(T) = T(T - 1)$, so $\mathrm{N}(f) - 1 = 7^2 - 1 = 2^4 \cdot 3$. It is easier to enumerate nonwitnesses than witnesses. Since T and $T - 1$ are linear, and $-1 \neq \square$ in

[3]This probabilistic heuristic has a small error related to Bayes' rule, which we don't discuss here.

$\mathbf{F}_7$, a Miller–Rabin nonwitness for f is a nonzero $a \in \mathbf{F}_7[T]$ of degree less than 2 such that $a^3 \equiv \pm 1 \bmod f$. By the Chinese remainder theorem this is equivalent to

$$a^3 \equiv 1 \bmod T \text{ and } a^3 \equiv 1 \bmod T - 1$$

or

$$a^3 \equiv -1 \bmod T \text{ and } a^3 \equiv -1 \bmod T - 1,$$

which means $a(0)^3 = 1$ and $a(1)^3 = 1$, or $a(0)^3 = -1$ and $a(1)^3 = -1$ in $\mathbf{F}_7$. The first pair of equations means $a(0)$ and $a(1)$ belong to $\{1, 2, 4\}$, while the second pair means $a(0)$ and $a(1)$ belong to $\{3, 5, 6\}$. Thus the number of such a is $9 + 9 = 18$. The proportion of Miller–Rabin nonwitnesses for f is $18/48 = 3/8 = .375 > 1/4$ and therefore the proportion of Miller–Rabin witnesses for f is $30/48 = 5/8 = .675$, which is less than 75%.

What we saw in this example is actually typical: the proportion of Miller–Rabin witnesses for every (monic) Carmichael polynomial in $\mathbf{F}_p[T]$ with only two irreducible factors is less than 75% except for a few examples when $p = 3$ or 5, in which case the proportion is 75%.

Theorem 5.6. *Let f be a product of two different monic irreducibles in $\mathbf{F}_p[T]$ with the same degree. The proportion of Miller–Rabin witnesses for f lies in the interval $(1/2, 3/4]$. The proportion is $3/4$ if and only if $p = 3$ or 5 and the irreducible factors of f are linear.*

Proof. Set $f = \pi_1\pi_2$ where π_1 and π_2 are different monic irreducibles with common degree d, so $\deg f = 2d$. Write $\mathrm{N}(f) - 1 = 2^e k$ where $e \geq 1$ and k is odd. Write $\mathrm{N}(\pi_1) - 1 = \mathrm{N}(\pi_2) - 1 = p^d - 1$ as $2^v\ell$ where $v \geq 1$ and ℓ is odd. Then

$$\mathrm{N}(f) - 1 = p^{2d} - 1 = (p^d - 1)(p^d - 1 + 2) = 2^v\ell(2^v\ell + 2) = 2^{v+1}(2^{v-1}\ell + 1)\ell, \tag{5.1}$$

so $e \geq v + 1 \geq 2$ and $\ell \mid k$.

Rather than count Miller–Rabin witnesses we will count Miller–Rabin nonwitnesses.

Case 1: $a^k \equiv 1 \bmod f$.

We will show

$$|\{a \bmod f : a^k \equiv 1 \bmod f\}| = \ell^2. \tag{5.2}$$

We have

$$a^k \equiv 1 \bmod f \Longleftrightarrow a^k \equiv 1 \bmod \pi_1 \text{ and } a^k \equiv 1 \bmod \pi_2.$$

For any cyclic group G of order M and $m \in \mathbf{Z}^+$, $|\{g \in G : g^m = 1\}| = (m, M)$. Taking for G the nonzero polynomials modulo π_j for $j = 1$ or 2, the number of solutions $a \bmod \pi_j$ to $a^k \equiv 1 \bmod \pi_j$ is $(k, \mathrm{N}(\pi_j) - 1) = (k, 2^v\ell) = \ell$ since k is odd and $\ell \mid k$. This proves (5.2) by the Chinese remainder theorem, which completes Case 1.

Case 2: $a^{2^i k} \equiv -1 \bmod f$ for some $i \in \{0, \ldots, e - 1\}$.

Recall that $e \geq v + 1$, so $v \leq e - 1$. The congruence $a^{2^i k} \equiv -1 \bmod f$ can only have a solution when $i < v$. Indeed, if $i \geq v$ then for $j = 1$ and 2 the number $\mathrm{N}(\pi_j) - 1 = 2^v\ell$ is a factor of $2^i k$, so $a \not\equiv 0 \bmod f \Rightarrow a^{2^i k} \equiv 1 \bmod f$ by Fermat's little theorem for moduli π_1 and π_2. For $0 \leq i \leq v - 1$, we will show

$$|\{a : a^{2^i k} \equiv -1 \bmod f\}| = 4^i\ell^2. \tag{5.3}$$

Claim: For $\pi = \pi_1$ or π_2, we have $a^{2^i k} \equiv -1 \bmod \pi$ if and only if $a \bmod \pi$ has order $2^{i+1}m$ where $m \mid \ell$.

Proof of claim: Let $a \bmod \pi$ have order A. If $a^{2^i k} \equiv -1 \bmod \pi$ then $a^{2^i k} \bmod \pi$ has order 2. Also the order of $a^{2^i k} \bmod \pi$ is $A/(2^i k, A)$, so $A = 2(2^i k, A)$. Letting 2^t be the highest

power of 2 dividing A, $t = 1 + \min(i, t)$, so $\min(i, t) = t - 1$. Thus $i = t - 1$, so $t = i + 1$ and $A = 2^{i+1}m$ for some odd m. Since A is a factor of $\mathrm{N}(\pi) - 1 = 2^v\ell$, we get $m \mid \ell$.

Conversely, suppose $a \bmod \pi$ has order $2^{i+1}m$ where $m \mid \ell$. Then $a^{2^i m} \not\equiv 1 \bmod \pi$ but $a^{2^{i+1}m} \equiv 1 \bmod \pi$, so $a^{2^i m} \equiv -1 \bmod \pi$ (the only residue mod π with order 2 is $-1 \bmod \pi$). Raising both sides to the k/m power (an odd power), we get $a^{2^i k} \equiv -1 \bmod \pi$.

For a cyclic group G of order M, and a positive factor D of M, the number of elements of G with order D is $\varphi(D)$. Applying this to the group of nonzero polynomials modulo π,

$$\begin{aligned} |\{a \bmod \pi : a^{2^i k} \equiv -1 \bmod \pi\}| &= \sum_{m \mid \ell} \varphi(2^{i+1}m) \\ &= \sum_{m \mid \ell} \varphi(2^{i+1})\varphi(m) \\ &= 2^i \sum_{m \mid \ell} \varphi(m) \\ &= 2^i \ell. \end{aligned}$$

The formula (5.3) follows from this by the Chinese remainder theorem, which completes Case 2.

The counts in Case 1 and Case 2 (as i runs from 1 to $v - 1$) cover disjoint possibilities, so the number of Miller–Rabin nonwitnesses for f is

$$\ell^2 + \sum_{i=0}^{v-1} 4^i \ell^2 = \ell^2 + \frac{4^v - 1}{3}\ell^2 = \frac{4^v + 2}{3}\ell^2. \tag{5.4}$$

As a reminder, v and ℓ come from $p^d - 1 = 2^v\ell$, where $\deg f = 2d$, so this count of Miller–Rabin nonwitnesses is entirely determined by $\deg f$ (and p).

By (5.1) and (5.4), the proportion of Miller–Rabin nonwitnesses for f is

$$\frac{(4^v + 2)\ell^2/3}{\mathrm{N}(f) - 1} = \frac{(4^v + 2)\ell^2/3}{2^{v+1}(2^{v-1}\ell + 1)\ell} = \frac{1}{3} \cdot \frac{4^v\ell + 2\ell}{4^v\ell + 2^{v+1}} = \frac{1}{3} \cdot \frac{1 + 2/4^v}{1 + 2/(2^v\ell)}. \tag{5.5}$$

For $v \geq 1$ and $\ell \geq 1$, this expression is less than $\frac{1}{3}(1 + 2/4) = \frac{1}{2}$ and greater than or equal to $\frac{1}{3}(1 + 2/4^v)/(1 + 2/2^v)$, which is $\frac{1}{4}$ at $v = 1$ and $v = 2$ and is greater than $\frac{1}{4}$ for $v \geq 3$. The conditions $v = 1$ or 2 and $\ell = 1$ correspond to $p^d - 1$ being 2 or 4, which means p is 3 or 5 and $d = 1$. So the proportion of Miller–Rabin nonwitnesses for f lies in $[1/4, 1/2)$ and equals $1/4$ if and only if $p = 3$ or 5 and $d = 1$. Switching from nonwitnesses to witnesses, the proportion of Miller–Rabin witnesses for f lies in $(1/2, 3/4]$ and equals $3/4$ if and only if $p = 3$ or 5 and $d = 1$. □

Corollary 5.7. *As f runs through the monic Carmichael polynomials in $\mathbf{F}_p[T]$ with exactly two irreducible factors of common degree d, its proportion of Miller–Rabin witnesses has the following limiting behavior:*

1. *if $p \equiv 1 \bmod 4$ then the proportion tends to $2/3$ as $d \to \infty$.*
2. *if $p \equiv 3 \bmod 4$ then the proportion tends to $2/3$ as $d \to \infty$ through even integers and to $1/2$ as $d \to \infty$ through odd integers.*

Proof. We use the notation from the proof of Theorem 5.6. Also we use $\mathrm{ord}_2(k)$, which denotes the exponent of the highest power of 2 that divides k, *e.g.*, $\mathrm{ord}_2(40) = 3$ and $\mathrm{ord}_2(k) = 1$ if and only if $k \equiv 2 \bmod 4$.

(1) Suppose $p \equiv 1 \bmod 4$. For any integer $c \equiv 1 \bmod 4$ with $c \neq 1$ and integer $m \geq 1$, $\mathrm{ord}_2(c^m - 1) = m + \mathrm{ord}_2(c-1)$. Therefore $v = \mathrm{ord}_2(p^d - 1) = d + \mathrm{ord}_2(p-1)$, so the proportion of Miller–Rabin nonwitnesses for f in (5.5) can be rewritten as

$$\frac{1}{3} \cdot \frac{1 + 2/4^{d+\mathrm{ord}_2(p-1)}}{1 + 2/(p^d - 1)}, \tag{5.6}$$

which tends to $\frac{1}{3}$ as $d \to \infty$. Thus the proportion of Miller–Rabin witnesses tends to $\frac{2}{3}$ as $d \to \infty$.

(2) If $p \equiv 3 \bmod 4$ and d is even then $p^2 \equiv 1 \bmod 4$, so

$$v = \mathrm{ord}_2(p^d - 1) = \mathrm{ord}_2((p^2)^{d/2} - 1) = \frac{d}{2} + \mathrm{ord}_2(p^2 - 1) = \frac{d}{2} + 1 + \mathrm{ord}_2(p+1).$$

Thus (5.5) equals

$$\frac{1}{3} \cdot \frac{1 + 2/4^{d/2+1+\mathrm{ord}_2(p+1)}}{1 + 2/(p^d - 1)}, \tag{5.7}$$

which tends to $\frac{1}{3}$ as $d \to \infty$ through even values, so the proportion of Miller–Rabin witnesses tends to $\frac{2}{3}$ as $d \to \infty$ through even values.

If $p \equiv 3 \bmod 4$ and d is odd then $p^d \equiv 3 \bmod 4$, so $p^d - 1 \equiv 2 \bmod 4$ and $v = 1$. Thus $\ell = (p^d - 1)/2$, so (5.5) becomes

$$\frac{1}{3} \cdot \frac{1 + 2/4}{1 + 2/(2\ell)} = \frac{\ell}{2(\ell+1)} = \frac{p^d - 1}{2(p^d + 1)} = \frac{1}{2} - \frac{1}{p^d + 1}.$$

Therefore the proportion of Miller–Rabin witnesses for f is

$$1 - \left(\frac{1}{2} - \frac{1}{p^d + 1}\right) = \frac{1}{2} + \frac{1}{p^d + 1},$$

which tends to $\frac{1}{2}$ as $d \to \infty$ through odd values. □

References

[1] R. Dedekind, Abriss einer Theorie der höheren Kongruenzen in Bezug auf einer reellen Primzahl-Modulus, *J. Reine Angew. Math.* **54** (1857), 1–26,

[2] M. Rosen, "Number theory in function fields," Springer–Verlag, New York, 2002.