4. THE TOO MANY PRIMES TEST

§4.1. Prime or Unit Values of a Composite Integer Polynomial

The material in this chapter was developed by me in teaching Galois Theory over many years at Macquarie University. It provides an additional test for primality over $\mathbb{Q}$ that can be quite useful.

If you substitute an integer into an integer polynomial you get an integer and products of polynomials give rise to products of integers. So if f(n) is prime you might expect that f(x) is prime over $\mathbb{Z}$ and hence prime over $\mathbb{Q}$. But it might be that f(x) is composite but one of its factors gives the value ± 1 when you substitute. However this cannot happen too many times because a polynomial a(x) of degree n can't give the same value for more than n values of x (let alone for integer values of x).

So a polynomial that gives a prime value (or a ± 1 value for that matter) for sufficiently many integers must be prime. But how many is sufficiently many?

If $a(x)$ is a non constant integer polynomial let **U(a(*x*))** be the number of integer values of x for which $a(x) = \pm 1$ and let **P(a(*x*))** be the number of integer values for which $a(x)$ is prime or ± 1. Clearly $U(a(x)) \leq P(a(x))$ for all integer polynomials. And if deg $a(x) = 1$ then $U(a(x)) \leq 2$.

Theorem 1: If $a(x)$ is an integer polynomial of degree n then $U(a(x)) \leq 2n$.
Proof: $a(x) - 1$ has at most n zeros as has $a(x) + 1$. Even if all these are integers and are distinct this would give at most $2n$ such values.

Lemma: If $a(x) = b(x)c(x)$ where neither factor is constant then $P(a(x)) \leq U(b(x)) + U(c(x))$.
Proof: If $a(n)$ is prime or ± 1 for some integer n then $b(n)$ or $c(n)$ is ± 1.

Theorem 2: If $a(x)$ is a composite integer polynomial of degree n then $P(a(x)) \leq 2n$.
Proof: Suppose $a(x) = b(x)c(x)$ where deg $b(x) = r \geq 1$ and deg $c(x) = s \geq 1$.
Then $P(a(x)) \leq U(b(x)) + U(c(x)) \leq 2r + 2s = 2n$.

This gives rise to the following simple test for primeness over $\mathbb{Q}$. An integer polynomial $a(x)$ of degree $n \geq 2$ which gives prime or ± 1 values for at least $2n + 1$

integer values of x is prime over $\mathbb{Q}$. However, except for quadratics, we can improve on this by reducing the number of values needed.

§4.2. Unit Values of an Integer Polynomial

Theorem 3: If $a(x) \in \mathbb{Z}[x]$ and $m, n \in \mathbb{Z}$ with $a(m) = 1$ and $a(n) = -1$ then $|m - n| \leq 2$.

Proof: As a polynomial in two variables
$a(x) - a(y) = (x - y)q(x, y)$ for some polynomial in x, y with integer coefficients.
Now $2 = a(m) - a(n) = (m - n)q(m, n)$ so $|m - n| = 1$ or 2.

If $a(x) \in \mathbb{Z}[x]$ we define its **PN string** as follows. Suppose $U(a(x)) = k$ and suppose that $a(x)$ takes ± 1 values for integers $n_1, n_2, ..., n_k$ where $n_1 < n_2 < ... < n_k$. The PN sequence is a sequence of P's and N's where the i'th symbol is P if $a(n_i) = 1$ and N if $f(n_i) = -1$.

Example 1: If $a(n_1) = a(n_2) = a(n_4) = f(n_5) = 1$ and $a(n_3) = -1$ and $a(n)$ is not 1 or -1 for any other integer value of x, then the PN sequence of $a(x)$ is PPNPP.

We define a PN sequence to be **mixed** if it contains at least one N and at least one P. The string PPNPP is mixed but PPPPP is not.

Theorem 4 (COOPER): If $n \geq 5$ there are no mixed PN sequences of length n.

Proof: There are 16 PN strings of length 4 but to satisfy Theorem 3 they must start and finish with the same symbol. This gives:

PPPP, PPNP, PNPP, PNNP, NPPN, NPNN, NNPN, NNNN

as the only possible PN strings of length 4.

A PN string of length 5 must begin with one of these and, because of Theorem 3 it must end with the same symbol as the first. This gives the following possibilities:

PPPPP, PPNPP, PNPPP, PNNPP, NPPNN, NPNNN, NNPNN, NNNNN

but again, in view of Theorem 3, we may eliminate PNPPP, PNNPP, NPPNN, NPNNN leaving:

PPPPP, PPNPP, NNPNN, NNNNN.

Now suppose a(x) has the string PPNPP. Then for some integers $n_1 < n_2 < n_3 < n_4 < n_5$, a($n_1$) = a($n_2$) = a($n_4$) = a($n_5$) = 1 and a($n_3$) = –1. In view of the Theorem 3, $n_1, \ldots, n_5$ must be 5 successive integers. So for some integer k, a(x) – 1 has zeros $k \pm 2$ and $k \pm 1$.

Hence
$a(x) - 1 = (x - k - 2)(x - k - 1)(x - k + 1)(x - k + 2)q(x)$ for some $q(x) \in \mathbb{Z}[x]$. Putting $x = k$ we get the contradiction $-2 = (-2)(-1).1.2.q(k) + 1$.

So PPNPP is impossible. Similarly NNPNN cannot arise. So the length of a mixed NP string is at most 4.

This gives the following upper bounds for $U(a(x))$.

deg a(x)	**U(a(x)) ≤**
1	2
2	4
3	4
4	4
$n > 4$	n

These upper bounds are the best possible because we can find polynomials where the degrees are as given in the second column.

Suppose $a(x) = b(x)c(x)$ where $1 \le \deg b(x) \le \deg c(x)$.

deg a	**deg b**	**deg c**	**U(b) ≤**	**U(c) ≤**	**P(a) ≤**
2	1	1	2	2	4
3	1	2	2	4	6*
4	1	3	2	4	8
	2	2	4	4	

5	1	4	2	4	8
	2	3	4	4	
6	1	5	2	5	
	2	4	4	4	8
	3	3	4	4	
$n > 6$	1	$n - 1$	2	$n - 1$	
	2	$n - 2$	4	$n - 2$	$n + 2$
	3	$n - 3$	4	$n - 3$	
	$r \geq 4$	$n - r \geq r \geq 4$	r	$n - r$	

In the next section we'll improve on this and show that if $a(x)$ is a composite cubic then $P(a(x)) \leq 5$.

§4.3. Prime or Unit Values of Integer Cubics

Lemma: Every sequence of 4 successive odd numbers, greater than 2, contains a composite integer.

Proof: The requirement that they all be greater than 2 is necessary because 1, 3, 5, 7 contains no composite number. But if $n > 2$ and none of n, $n + 2$, $n + 4$, $n + 6$ are composite then they must all be prime. Now at least one of this sequence is a multiple of 3 and so must be ± 3. This multiple of 3 can't be $n + 2$ or $n + 4$ because ± 1 aren't prime. So $n = \pm 3$, but then both possibilities lead to a contradiction.

Theorem 7 (COOPER): If $a(x)$ is a composite integer cubic then $P(a(x)) \leq 5$.

Proof: Suppose $a(x) = b(x)c(x)$ where $b(x)$ is an integer polynomial of degree 1 and $c(x)$ is an integer quadratic. We know that $P(a(x)) \leq 6$. Suppose that $P(a(x)) = 6$. Then $b(x)$ is ± 1 for 2 integer values of x and $c(x)$ is ± 1 for 4 values of x. Also, these 6 values must be distinct and when one factor is ± 1 the other factor must be prime or ± 1. The PN pattern for $c(x)$ must be PNNP or NPPN. Suppose, without loss of generality, that it is PNNP. Then, by Theorem 3, $c(x)$ is ± 1 for 4 consecutive integer values of x, say k, $k + 1$, $k + 2$, $k + 3$.

Let $A(x) = a(x + k)$, $B(x) = b(x + k)$ and $C(x) = c(x + k)$. Then $A(x) = B(x)C(x)$ and $C(x) = \pm 1$ for $x = 0, 1, 2, 3$.
In fact, since the PN pattern of $C(x)$ is PNNP,

$$C(0) = C(3) = 1 \text{ and } C(1) = C(2) = -1.$$

It's easy to show that $C(x) = x^2 - 3x + 1$.

Now $B(x) = \pm 1$ for 2 integer values of x, say m, n where $m < n$. Clearly $B(m) \neq B(n)$ and without loss of generality we may assume that $B(m) = -1$ and $B(n) = 1$.

Let $B(x) = cx + d$ where $c > 0$.
Since $cm + d = -1$ and $cn + d = 1$, we have $c(n - m) = 2$.
Thus $c = 1$ or 2.

Case 1: $c = 1$: B(x) is prime, or ± 1 for $x = 0, 1, 2, 3$ and these 4 values are: d, $d + 1$, $d + 2$, $d + 3$. Two of these are even and so must be ± 2. Clearly this is impossible.
Case 2: $c = 2$: Then $n - m = 1$ and $d = -1 - 2m$.
Now $\{m, m + 1\}$ is disjoint from $\{0, 1, 2, 3\}$

$$\text{so } m \geq 4 \text{ or } m \leq -2.$$

If $m \geq 4$ then $d \leq -9$. Now B(x) is prime, or ± 1 for $x = 0, 1, 2, 3$ and these 4 prime or ± 1 values are:

$$d, d + 2, d + 4, d + 6.$$

At least one of these is a multiple of 3 and so must be ± 3. But this would require $d = -9$, which is not prime. So this case cannot arise.

If $m \leq -2$ then $d \geq 3$ and by a similar argument we again get a contradiction.

PRIMENESS TEST 7: Too Many Primes Test
Theorem 8: (COOPER): If $f(x) \in \mathbb{Z}[x]$ has at least as many prime or ± 1 values for integer x as the target shown in the last column then $f(x)$ is prime over $\mathbb{Q}$.

deg f	P ≤	Target for prime-ness
1	2	3
2	4	5
3	5	6
4	8	9
5	8	9
$n > 5$	$n + 2$	$n + 3$

These values are best possible since one can find composite integer polynomials a(x) for which P(a(x)) is equal to the upper bound given in the middle column.

Example 2: The polynomial a(x) = $x^3 - x^2 - 3x + 1$ is prime over $\mathbb{Q}$ since it has at least 6 values which are prime or ± 1:

n	–3	–2	–1	0	1	2	3	4
a(n)	–26	–5	2	1	–2	–1	10	37
prime or unit?	×	√	√	√	√	√	×	√

Example 3: The polynomial $f(x) = x^8 - 5x^6 + 8x^2 + 13$ is prime over $\mathbb{Q}$ since it has at least 11 values which are prime or ± 1:

n	***f* (*n*)**	**prime or unit?**
± 6	1446637	√
± 5	312713	×
± 4	45197	√
± 3	3001	√
± 2	– 19	√
± 1	17	√
0	13	√

EXERCISES FOR CHAPTER 4

Exercise 1: Determine which of the following are prime, using the too many primes test.
(i) $a(x) = x^3 + 2x^2 - 7x - 1$;
(ii) $a(x) = x^4 - 3x^3 + 4x - 1$;
(iii) $a(x) = x^5 - 5x^4 + 17$.

Exercise 2: (a) Find integer polynomials $a(x)$, $b(x)$ of degrees 2 and 3 respectively for which
$U(a(x)) = U(b(x)) = 4$.
(b) Find a composite integer polynomial $d(x)$ of degree 4 for which $P(d(x)) = 8$.

SOLUTIONS FOR CHAPTER 4

Exercise 1:

(i)

n	0	1	2	3	–1	–2
$f(n)$	–1	–5	1	23	7	13
prime or unit?	√	√	√	√	√	√

(ii)

n	0	1	2	3	4	–1	–2	–3	–4	–5
$f(n)$	–1	1	–1	11	79	–1	31	149	431	979
prime or unit?	√	√	√	√	√	√	√	√	√	×

(iii)

n	$f(n)$	**prime or unit**
– 5	1087	√
– 4	499	√
– 3	185	
– 2	43	√
– 1	5	√
0	– 13	√
1	– 11	√
2	– 5	√
3	23	√
4	115	
5	337	√

Question 2:

(a) The PN pattern for $a(x)$ must contain two N's and two P's and clearly NPNP or PNPN are impossible for a quadratic. Suppose that the PN pattern for $a(x)$is PNNP. Then the 4 integer values of x for which $a(x) \in$ T must be consecutive.

Suppose a(0) = a(3) = 1 and a(1) = a(2) = –1.

It is easy to show that $a(x) = x^2 - 3x + 1$ satisfies these conditions.

Suppose the PN pattern for b(x) is PPNP. The first 3 integer values of x for which b(x) $\in$ T must be consecutive and the fourth must be one or two beyond the third.

Suppose that b(0) = b(1) = b(3) = 1 and b(2) = –1.

It is easy to show that $b(x) = kx(x - 1)(x - 3) + 1$ for some integer k and since b(2) = –1,we must have $k = -1$. Hence $b(x) = x^3 - 4x^2 + 3x + 1$ satisfies these conditions.

(b) Clearly d(x) must be a product of two quadratics, each of which takes values in T for 4 integer values of x. However these values must be distinct.

Let's take $a(x) = x^2 - 3x + 1$ for the first factor. This takes values in T for x = 0, 1, 2, 3.

By replacing x by $x + 4$ we get a quadratic that takes values in T for x = –4, –3, –2, –1.

This second factor is

$$(x + 4)^2 - 3(x + 4) + 1 = x^2 + 5x + 5.$$

So let $d(x) = (x^2 - 3x + 1)(x^2 + 5x + 5)$. We must now check that, for these 8 values, when one factor is in T the

other is in P and that indeed d(x) is in P. As this table shows this is indeed the case.

x	**–4**	**–3**	**–2**	**–1**	**0**	**1**	**2**	**3**
d(x)	29	–19	–11	5	5	–11	–19	29