COUNTING THE ROOTS OF A POLYNOMIAL IN A RING MODULO n

Curt Minich

Master's Thesis
(MAT 600 - Elements of Research)
August 16, 1994

Shippensburg University

ACKNOWLEDGEMENTS

The author would like to acknowledge Dr. Leonard Jones of Shippensburg University for his invaluable suggestions, criticisms and guidance.

ABSTRACT

While a polynomial of degree m has at most m distinct roots in a field, it may have more than m roots in the ring of integers modulo n. The objective of this research is to describe a method for counting the number of roots of a polynomial in a ring modulo n without having to calculate each root. This research extends the work of Scott Fabbri, who examined polynomials of the form $x^2 - a^2 \equiv 0$ in $\mathbb{Z}/n\mathbb{Z}$ where a^2 divides n. This work examines polynomials of the same form where a^2 and n are relatively prime. A rule is stated which tabulates the number of roots to any such polynomial and a method for building a polynomial with a given number of roots is also detailed.

This research examines polynomials of the form $x^2 - a^2 \equiv 0$ in $\mathbb{Z}/n\mathbb{Z}$ where a^2 and n are relatively prime. Three main results will be demonstrated:

1/ Given n, the number of roots can be predicted.
2/ The number of roots for any given n is always a power of two.
3/ A rule for building a polynomial with a given number of roots

is specified.

LEMMA 1. When (a,n) = 1, $x^2 - a^2 \equiv 0 \pmod{n}$ has the same number of roots as $x^2 - 1 \equiv 0 \pmod{n}$.

Proof: Let y be a root to $x^2 - a^2 \equiv 0 \pmod{n}$

then $y^2 \equiv a^2 \pmod{n}$

$\Leftrightarrow y^2 (a^{-1})^2 \equiv 1 \pmod{n}$

$\Leftrightarrow (ya^{-1})^2 - 1 \equiv 0 \pmod{n}$

So ya^{-1} is a corresponding root for $x^2 - 1 \equiv 0 \pmod{n}$.

Furthermore ya^{-1} is unique because for any root z to $x^2 - a^2 \equiv 0 \pmod{n}$ where z does not equal y, za^{-1} does not equal ya^{-1}

Next, given n, it is determined how many roots there are to $x^2 - 1 \equiv 0 \pmod{n}$. First , note that 1 and n-1 are always roots since $1^2 - 1 \equiv 0 \pmod{n}$ and $(n-1)^2 - 1 \equiv 0\ n(n-2) \equiv 0 \pmod{n}$.

Since $x^2 - 1 \equiv 0 \pmod{n}$ can be rewritten as $x^2 \equiv 1 \pmod{n}$, finding roots is equivalent to finding elements of order 2 in the multiplicative group of $\mathbb{Z}_n$ (that is, $\mathbb{Z}^*_n$). Note that 1, the unity, is also a root. Note that $\mathbb{Z}^*_n$ is isomorphic to $\mathbb{Z}^*_{q_1^{\alpha_1}} \times \mathbb{Z}^*_{q_2^{\alpha_2}} \times \mathbb{Z}^*_{q_3^{\alpha_3}} \times \ldots \times \mathbb{Z}^*_{q_n^{\alpha_n}}$ where $n = q_1^{\alpha_1} q_2^{\alpha_2} q_3^{\alpha_3} \ldots q_n^{\alpha_n}$ is the prime factorization of n. Gauss shows that:

a/ if p is an odd prime, then $\mathbb{Z}^*_{p^m}$ and $\mathbb{Z}^*_{2p^m}$ are cyclic groups of order $k=(p-1)p^{m-1}$ for all natural numbers m and both are isomorphic to $\mathbb{Z}_k$, which has one element of order two, namely k/2.

b/ if p = 2, then

$\mathbb{Z}_2^*$ is cyclic of order $2^0 = 1$.

$\mathbb{Z}_{2^2}^*$ is cyclic of order $2^1 = 2$ and it is isomorphic to $\mathbb{Z}_2$, which has one element of order two, namely 1.

$\mathbb{Z}_{2^m}^*$ is the direct product of a subgroup of order 2 and a cyclic subgroup of order 2^{m-2} and it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{m-2}$,

which has three elements of order two (ie. $(0, \frac{m-2}{2})$, $(1, \frac{m-2}{2})$, and (1,0)).

Therefore the number of elements of order two in $\mathbb{Z}_n^*$ is dependent on the number of different prime factors of n and the power of 2 in the prime factorization of n. Gauss' work and Lemma 1 lead to the following theorem concerning the number of roots to $x^2 - 1 \equiv 0 \pmod{n}$. Keep in mind that the unity satisfies the polynomial in every case.

THEOREM 1. Let z be the number of different odd prime factors of n, let r be the number of roots and let m be the highest power of two that divides n.

i/ $r = 2^z$ if $m = 0$ or 1
ii/ $r = 2^{z+1}$ if $m = 2$
iii/ $r = 2^{z+2}$ if $m \geq 3$

Obviously, the number of roots is always a power of two. Lemma 1 proves that these formulas apply to polynomials of the form $x^2 - a^2 \equiv 0 \pmod{n}$ where (a,n)=1. Armed with Theorem 1, a rule for building a polynomial with a given number of roots can now be specified in the next theorem.

THEOREM 2. For any given number of roots, r, which must be a power of two, n can be specified for which the equation, $x^2 - a^2 \equiv 0 \pmod{n}$, will have r roots.

Different rules apply to the following cases:

a/ If it is desired for n to be odd, construct n as the product of $\log_2 r$ odd prime factors (each having any power).

Example- To construct a polynomial with 8 roots, take the product of 3 ($\log_2 8$) odd prime factors as n such as $n = 3 \cdot 5 \cdot 7 = 105$.

b/ If n must be even but not divisible by 4, construct n as the product of $\log_2 r$ odd prime factors (each having any power) and 2.

Example- To construct a polynomial with 16 roots where n is even but not divisible by 4, construct n as the product of 4 ($\log_2 16$) odd prime factors and the number 2 such as $n = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 2 = 2310$.

c/ If n must be even and divisible by 4, construct n as the product of $\log_2 r$-1 odd prime factors (each having any power) and four.

Example- To construct a polynomial with 32 roots where n is even and divisible by 4, construct n as the product of 4 ($\log_2 32$-1) odd prime factors with the number 4 such as $n = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 4 = 4620$.

d/ If n must be even and divisible by 2 to some power greater than 2, construct n as the product of $\log_2 r$-2 odd prime factors (each having any power) and 2 to the necessary power.

Example- To construct a polynomial with 64 roots where n is even and divisible by 16, construct n as the product of $\log_2 64$-2 = 4 odd prime factors and the number 16 such as $n = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 16 = 1\ 8480$.

According to the rules above, the smallest value n, for which the polynomial, $x^2 - a^2 \equiv 0 \pmod n$, has:

8 roots is $3 \cdot 8 = 24$.
16 roots is $3 \cdot 5 \cdot 8 = 120$.
32 roots is $3 \cdot 5 \cdot 7 \cdot 8 = 840$.
64 roots is $3 \cdot 5 \cdot 7 \cdot 11 \cdot 8 = 9240$.

128 roots is $3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 8 = 120120$.

Each "smallest" value of n is found by taking the product of the smallest consecutive odd primes and 2^3. Each odd prime "contributes" a factor of two in the resulting number of roots. A factor of four is "contributed" towards the number of roots by 2^3.

FUTURE RESEARCH

While this theory explains a method for counting the number of roots to $x^2 - a^2 \equiv 0 \pmod{n}$ where a and n are relatively prime, it could be extended to include a method for counting the roots when a and n are not relatively prime and a^2 does not divide n. It is conjectured that the roots can be counted similarly by counting odd prime factors of n and noting two's divisibility into n as long as the common factors (except for two) between a and n are ignored. For example, with a=5 and n=60, 5 is a common factor between a and n. Although the prime factorization of 60 includes two odd prime factors, 3 and 5, and 2^2, the common factor, 5, is ignored so there should be 4 roots according to Theorem 1, case ii. Even if two to some power is a common factor of a and n, its divisibility into n still affects the number of roots. As another example, let a=165 which has 3, 5 and 11 as factors. Let n=10920, which has the following factors: 3, 5, 7, 13 and 2^3. Ignoring the common factors of 3 and 5, n has two remaining odd prime factors and a factor of 2^3. Using Theorem 1, case iii, there are 16 roots to the polynomial.

REFERENCES

Schilling, Otto F. and Piper, Stephen W. Basic Abstract Algebra. Boston: Allyn and Bacon, 1975.

TECHNICAL INFORMATION

This paper was originally typeset on an Apple Macintosh computer using Microsoft Word with Equation Editor. Body text is in New York 12 point, with symbols set in Symbol 12 point. Superscripts and subscripts are set in point according to level. A computer

program written in ThinkPascal was used to tabulate the number of roots and to calculate the actual roots to the polynomials. It is included as an attachment.

ATTACHMENT

Given: $x^2 - 1 \equiv 0 \pmod{n}$

n	# of roots	n	# of roots	n	# of roots
1	1	101	2	1001	8
2	1	102	4	1002	8
3	2	103	2	1003	4
4	2	104	8	1004	4
5	2	105	8	1005	4
6	2	106	2	1006	8
7	2	107	2	1007	2
8	4	108	4	1008	4
9	2	109	2	1009	16
10	2	110	4	1010	2
11	2	111	4	1011	4
12	4	112	8	1012	4
13	2	113	2	1013	8
14	2	114	4	1014	2
15	4	115	4	1015	4
16	4	116	4	1016	8
17	2	117	4	1017	4
18	2	118	2	1018	2
19	2	119	4	1019	2
20	4	120	16	1020	16
21	4	121	2	1021	2
22	2	122	2	1022	4
23	2	123	4	1023	8
24	8	124	4	1024	4
25	2	125	2	1025	4
26	2	126	4	1026	4
27	2	127	2	1027	4
28	4	128	4	1028	4
29	2	129	4	1029	4
30	4	130	4	1030	4
31	2	131	2	1031	2

32	4	132	8	1032	16
33	4	133	4	1033	2
34	2	134	2	1034	4
35	4	135	4	1035	8
36	4	136	8	1036	8
37	2	137	2	1037	4
38	2	138	4	1038	4
39	4	139	2	1039	2
40	8	140	8	1040	16
41	2	141	4	1041	4
42	4	142	2	1042	2
43	2	143	4	1043	4
44	4	144	8	1044	8
45	4	145	4	1045	8
46	2	146	2	1046	2
47	2	147	4	1047	4
48	8	148	4	1048	8
49	2	149	2	1049	2
50	2	150	4	1050	8
51	4	151	2	1051	2
52	4	152	8	1052	4
53	2	153	4	1053	4
54	2	154	4	1054	4
55	4	155	4	1055	4
56	8	156	8	1056	16
57	4	157	2	1057	4
58	2	158	2	1058	2
59	2	159	4	1059	4
60	8	160	8	1060	8
61	2	161	4	1061	2
62	2	162	2	1062	4
63	4	163	2	1063	2
64	4	164	4	1064	16
65	4	165	8	1065	8
66	4	166	2	1066	4
67	2	167	2	1067	4
68	4	168	16	1068	8
69	4	169	2	1069	2
70	4	170	4	1070	4
71	2	171	4	1071	8

72	8	172	4	1072	8
73	2	173	2	1073	4
74	2	174	4	1074	4
75	4	175	4	1075	4
76	4	176	8	1076	4
77	4	177	4	1077	4
78	4	178	2	1078	4
79	2	179	2	1079	4
80	8	180	8	1080	16
81	2	181	2	1081	4
82	2	182	4	1082	2
83	2	183	4	1083	4
84	8	184	8	1084	4
85	4	185	4	1085	8
86	2	186	4	1086	4
87	4	187	4	1087	2
88	8	188	4	1088	8
89	2	189	4	1089	4
90	4	190	4	1090	4
91	4	191	2	1091	2
92	4	192	8	1092	16
93	4	193	2	1093	2
94	2	194	2	1094	2
95	4	195	8	1095	8
96	8	196	4	1096	8
97	2	197	2	1097	2
98	2	198	4	1098	4
99	4	199	2	1099	4
100	4	200	8	1100	8

```
program mathresearch1;
    {This ThinkPascal program calculates and lists the roots to the }
    {polynomial x^2 - a^2 ≡ 0 (mod n) in ℤ/nℤ. It also computes the    }
    {number of roots to the polynomial. The values of a and n can }
    {easily be changed within the program. }
var
    a2,             {The value of a squared}
    n,              {The value of n, that is the modulo}
    root,           {The value of a calculated root to the polynomial}
    root2minusa2,   {The value of x squared minus a squared}
```

```
      rootcounter       {The number of roots} : longint;
begin
      showtext;
      a2:=1;
      for n:=1 to 1000 do
            begin
                  rootcounter := 0;
                  if (n mod a2 <> 0) or (a2 = 1) then
                        write('n is :', n);
                  for root := 1 to n do
                        begin
                              root2minusa2 mod n = 0) then
                                    begin
                                          root2minusa2:=(root*root)-a2;
                                          write(root);
                                    end;
                        end;
                  write('number of roots=',rootcounter);
                  writeln;
            end;
end.
```