Infinite Period? PhL 7.10.13

How do you compute the period of some f(x) other than Maple brute force? I never really found a way, though looked down some Avenues here. Also, still not sure there are no nice f(x) which has an *infinite* period. I managed to work around not knowing the answers to these questions. I wanted to say something about the period of the CRC polynomial but decided to say just that it is probably very large.

New question. **Are there polynomials which have no period ?** That is to say

f(x) for which there exists no n>1 such that Rem[$(x^n-1)/f(x)$] ≠ 0.

1. We know this is true of $f(x) = x^i F(x)$, for example.

2. We know that if f(x) is a min poly for some GF(q), then there does exist such an n ≤ q-1.

So if we could show that f(x) was not a min poly for any GF(q), maybe that would be convincing.

Question: How do I know that $(x^n-1)/x$ has a remainder? $(x^n -1) = q(x)x + r(x)$. Here q(x) must have a term of degree x^{n-1} . Write $q(x) = Ax^{n-1} + Bx^{n-2} + F$

$(x^n -1) = Ax^n + Bx^{n-1} + ... + Fx$ cannot balance against the -1. Contradiction so need r(x) ≠ 0

Plan A. Suppose

$g(x)h(x) = x^n-1 = 1 + x^n$ GF2 only.

Then either g(1) = 0, h(1) = 0, or both.

Try general form

$g = g_0 + g_1x + g_2x^2 + ...g_sx^s$
$h = h_0 + h_1x + h_2x^2 + ...h_rx^r$

$gh = 1 + x^n = g_0h_0 + g_sx^s h_rx^r$ + intermediate terms

Need r+s = n, $g_sh_r = 1$, $g_0h_0 = 1$, all intermediate terms have even coefficients so 0.

c(x) = a(x) b(x) $\qquad c_s = \sum_{j=\max(0,s-A)}^{\min(s,B)} (a_{s-j} \otimes b_j)$.

Plan B. Suppose f(x) is irreducible in GF(2) and non-linear.

Plan C

Definition 4.2. *The* period of a polynomial $C(D)$ *is the least positive number* T *such that* $C(D)|(1 - D^T)$.

The period of a polynomial is easily calculated by division of 1 by $C(D)$ and continuing until the we receive the first remainder of the form $1 \cdot D^N$. Then the period is $T = N$.

Example 4.6. *Calculate the period of the polynomial* $C(D) = 3 + D^2$ *in* $\mathbb{F}_5$.

Solution: *We divide 1 by* $C(D)$ *and cancel out the lowest degree terms. The first reminder of the form* $1 \cdot D^N$ *indicate the period. Long division written in the following form:*

$$\begin{aligned} 1 &= 2 \cdot (3 + D^2) + (-2D^2) \\ 3D^2 &= D^2 \cdot (3 + D^2) + (-D^4) \\ 4D^4 &= 3D^4 \cdot (3 + D^2) + (-3D^6) \\ 2D^6 &= 4D^6 \cdot (3 + D^2) + (-4D^8) \end{aligned}$$

The remainder $(-4D^8) = D^8$ *has the required form* $1 \cdot D^N$. *The period of* $C(D)$ *is* 8.

Plan D

3.3 The order of σ

We can now calculate the order of $\sigma \restriction E$ for a generalized eigenspace E in the decomposition. For any element u in the regular part of the decomposition, define the *period* of u, in symbols per u, to be the least $i > 0$ such that $\sigma^i(u) = u$. Recall that the period of an irreducible polynomial τ is the least $p > 0$ such that $x^p + 1 = 0 \pmod{\tau}$. Thus, the period of a polynomial is the order of any of its roots in the multiplicative subgroup of a splitting field, and in particular divides $2^d - 1$ where d is the degree of τ. The period can be calculated by factoring $2^d - 1 = p_1^{e_1} \ldots p_k^{e_k}$ and then finding the least exponents c_i such that $p = p_1^{c_1} \ldots p_k^{c_k}$ satisfies $x^p + 1 = 0 \pmod{\tau}$. This requires essentially only a fast polynomial exponentiation algorithm with a fixed modulus τ; see, for example, [9]. Incidentally, for small-degree polynomials a brute force calculation based on shift-register sequences seems to be more efficient. We write $C_m \in \mathbb{F}_2[x]$ for the mth cyclotomic polynomial.

degree of τ. The period can be calculated by factoring $2^d - 1 = p_1^{e_1} \ldots p_k^{e_k}$ and then finding the least exponents c_i such that $p = p_1^{c_1} \ldots p_k^{c_k}$ satisfies $x^p + 1 = 0 \pmod{\tau}$. This requires essentially only a fast polynomial exponentiation algorithm with a fixed modulus τ; see, for example, [9]. Incidentally, for small-degree polynomials a brute force calculation based on shift-register sequences seems to be more efficient. We write $C_m \in \mathbb{F}_2[x]$ for the mth cyclotomic polynomial.

This seems to be saying that the period of any polynomial must divide $2^d - 1$. I think they are just saying that you have to find some GF(p^m) which does the trick, so maybe only try such values in a search.

I tried $n = 2^m - 1$ up to n = 4095 and could not divide my CRC-32 into x^n-1, and it is very slow at those numbers.

Conclusion: I don't think there is any easy way to find n for a given f(x).

Fact: If some monic f(x) is a min poly for some GF(q), then it must divide $x^{q-1} - 1$. If you find that f(x) does not divide $x^{q-1} - 1$, then you know it is not a min poly for that GF(q). You can keep testing higher values of q. A min poly must be irreducible I know. And the CRC one is irreducible. The question is: is it a min poly of some GF(q) ?

> The IEEE 802.3 standard adopts the CRC polynomial:
> $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$
> (this is irreducible, but not primitive). We represent this polynomial as a 32-bit hexadecimal number 0x82608EDB.

IN any event, I know that there is no n up to 1573 that works, so n < this would be OK.

Comment: Since the CRC has order 32, you would have to get to GF(2^{32}) just to have a min poly of that degree! Then you are testing x^n-1 for $n \geq 2^{32}$= 4,294,967,296. So if this CRC is a min poly, you have to go way out there before you can even start looking for a viable min poly! This field has 4 billion roots.