

Re: irreducible polynomial in $Z_7[t]$ roots of which are primitive in $GF(49)$

Re: irreducible polynomial in $Z_7[t]$ roots of which are primitive in $GF(49)$

Source: <http://sci.tech-archive.net/Archive/sci.math/2008-11/msg01698.html>

- *From:* Pink Pig <bill@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 14 Nov 2008 15:16:29 -0800 (PST)
-

On Nov 14, 4:28 pm, anonymous.rubbert...@xxxxxxxxxx wrote:

On Nov 14, 4:06 pm, Derek Holt <ma...@xxxxxxxxxxxxxxxx> wrote:

On 14 Nov, 13:22, anonymous.rubbert...@xxxxxxxxxx wrote:

On Nov 14, 7:57 am, Kenneth Bull
<kenneth.b...@xxxxxxxxxx> wrote:

How to find an irreducible polynomial in
 $Z_7[t]$ roots of which are
primitive in $GF(49)$ >

Primitives in $GF(p^n)$ are primitive $(p^n - 1)$ th roots of
unity; so to
get a polynomial in $Z_p[t]$ whose roots are primitives in
 $GF(p^n)$, try
a polynomial whose splitting field is the degree n unramified
extension of Z_p . In your case, I think the 48th ($48 = 7^2 -$
 1)
cyclotomic polynomial does it.

The 48th cyclotomic polynomial is $x^{16} - x^8 + 1$, and its
factorization over Z_7 is

Re: irreducible polynomial in $Z_7[t]$ roots of which are primitive in $GF(49)$

$$\langle x^2 + x + 3 \rangle * \langle x^2 + 2x + 3 \rangle * \langle x^2 + 2x + 5 \rangle * \langle x^2 + 3x + 5 \rangle * \\ \langle x^2 + 4x + 5 \rangle * \langle x^2 + 5x + 3 \rangle * \langle x^2 + 5x + 5 \rangle * \langle x^2 + 6x + 3 \rangle.$$

Derek Holt

Then I suppose those quadratic factors are the irreducible polynomials that the OP is looking for.

Any quadratic whose discriminant is a quadratic nonresidue of 7 will do. So, if the desired quadratic is $x^2 + b^*x + c$, you want the values of b and c such that $b^2 - 4^*c$ is a nonresidue of 7. The nonresidues of 7 are 3,5,6. With $b == 1,6$, you need to solve the equations $1 - 4^*c == 3,5,6 \pmod{7}$, which is the same as $2 - c == 6,3,5 \pmod{7}$, which gives $c == 3,6,4$, which gives, in addition to the above list, $x^2 + x + 4$ and $x^2 + 6^*x + 4$. With $b == 2,5$, you need to solve the equations $4 - 4^*c == 3,5,6 \pmod{7}$, which is the same as $1 - c == 6,3,5 \pmod{7}$, which gives $c == 2,5,3$, which gives, in addition to the above list, $x^2 + 2^*x + 2$ and $x^2 + 5^*x + 2$. With $b == 3,4$, you need to solve the equations $2 - 4^*c == 3,5,6 \pmod{7}$, which is the same as $4 - c == 6,3,5 \pmod{7}$, which gives $c == 5,1,6$, which gives, in addition to the above list, $x^2 + 3^*x + 1$, $x^2 + 4^*x + 1$, $x^2 + 3^*x + 6$ and $x^2 + 4^*x + 6$. There's also the case $b == 0$, in which case $-4^*c == 3,5,6 \pmod{7}$, i.e. $-c == 6,3,5 \pmod{7}$, i.e. $c == 1,4,2$, giving another three quadratics, $x^2 + 1$, $x^2 + 2$ and $x^2 + 4$.

There are 42 elements in $GF(49)$ which are not in $GF(7)$, and each is the root of a quadratic, namely if e is one of these values, then $(x - e)^*(x - e^7)$ evaluates to a polynomial in $GF(7)$. These 42 elements can thus be paired as (e, e^7) in essentially 21 distinct ways, corresponding to the 21 quadratics in $GF(7)$ which are irreducible. Note that $b = e + e^7$ satisfies $b^7 = b$, which shows that b is in fact in $GF(7)$; similarly $c = e^*e^7 = e^8$ satisfies $c^7 = c$, which shows that c is in $GF(7)$.

It looks like Derek's list includes those quadratics whose roots are also primitive roots of $GF(49)$ — in each case, the constant term is one of the primitive roots of 7 — i.e. either 3 or 5. The other 13 quadratics all have constant terms which are not primitive roots of 7.

The above argument can be extended to quadratics in either $GF(p)$ or $GF(p^2)$. Specifically, the number of quadratics which solve the corresponding problem is $p^*(p-1)/2$.

.