MathGroup Archive 2005

[Date Index] [Thread Index] [Author Index]

Search the Archive

go

Re: primitive polynomials

To: mathgroup at smc.vnet.net

Subject: [mg55902] Re: [mg55866] primitive polynomials

From: Daniel Lichtblau <danl at wolfram.com>

Date: Sat, 9 Apr 2005 03:55:59 -0400 (EDT)

References: <200504080536.BAA25150@smc.vnet.net>

Sender: owner-wri-mathgroup at wolfram.com

```
xxxxyz at abv.bg wrote:
> Hi,
>
> How can I check if a given polynomial is primitive in GF(2)?
>
> Thanks.
```

Here is code adopted from

http://forums.wolfram.com/mathgroup/archive/1998/Nov/msg00194.html

We assume at the start that the polynomial is irreducible modulo the prime in question. That can be tested as below.

```
isIrreducible[x_, poly_, p_] := Module[
   {fax},
   If [!PrimeQ[p] || !PolynomialQ[poly,x] || Variables[poly]=!={x},
     Return[False]];
   fax = FactorList[poly,Modulus->p];
   Length[fax]==2 && fax[[2,2]]==1
   ]
```

For primitive testing we need to know if powers of x are equivalent to 1 modulo certain factors of p^degree-1, where degree is the degree of the polynomial in question.

```
<<Algebra`

isPrimitive[x_, poly_, p_, deg_] := Catch[Throw[Module[
   {fax=(p^deg-1)/Map[First,FactorInteger[p^deg-1]]},
   For [j=1, j<=Length[fax], j++,
     If [PolynomialPowerMod[x,fax[[j]],{poly,p}]===1, Throw[False]];
     ];
   True
   ]]]
```

Here is an example from the note at that URL. We work modulo 293. For your situation you would set the 'p' parameter to 2.

```
p = 293;
deg = 15;

poly = 38 + 117*x + 244*x^2 + 234*x^3 + 212*x^4 + 142*x^5 + 103*x^6 +
   60*x^7 + 203*x^8 + 124*x^9 + 183*x^10 + 96*x^11 + 225*x^12 +
   123*x^13 + 251*x^14 + x^15;
```

First we'll check that it is irreducible (it is, because as per that note it was manufactured in such a way as to be irreducible).

```
In[14]:= isIrreducible[x,poly,p]
Out[14]= True

In[15]:= isPrimitive[x,poly,p,deg]
Out[15]= False
```

So this is not a primitive polynomial. Note that we can construct such a polynomial by testing, instead of x, terms such as x+1, x+2,...

```
In[16]:= isPrimitive[x+1,poly,p,deg]
```

```
poly with x replaced by x-2.

poly2 = poly /. x->x-2;

In[19]:= isPrimitive[x,poly2,p,deg]
Out[19]= True

In addition to the above URL there is information on finite field
polynomial manipulation at

http://forums.wolfram.com/mathgroup/archive/2003/Mar/msg00494.html


Daniel Lichtblau
Wolfram Research
```

References:

primitive polynomials

From: "xxxxyz@abv.bg" <xxxxyz@abv.bg>

- Prev by Date: **Re: Having trouble with substitution tile at higher iteration levels--> takes forever!**
- Next by Date: **Re: Replacement gyrations**
- Previous by thread: **primitive polynomials**
- Next by thread: **Sorting complex points**

Products
Wolfram|One
Mathematica
Wolfram|Alpha Notebook Edition
Wolfram|Alpha Pro
Mobile Apps
Finance Platform
System Modeler
Wolfram Player
Wolfram Engine
WolframScript
Wolfram Workbench
Volume & Site Licensing
Enterprise Private Cloud
Application Server
VIEW ALL...

Services
Technical Consulting
Corporate Consulting

For Customers
Online Store
Product Registration
Product Downloads
Service Plans Benefits
User Portal
Your Account

Support
Support FAQ
Customer Service
Contact Support

Learning
Wolfram Language Documentation
Wolfram Language Introductory Book
Get Started with Wolfram
Fast Introduction for Programmers
Fast Introduction for Math Students
Webinars & Training
Wolfram U
Summer Programs
Videos
Books

Public Resources
Wolfram|Alpha
Demonstrations Project
Resource System
Connected Devices Project
Wolfram Data Drop
Wolfram + Raspberry Pi
Wolfram Science
Computer-Based Math
MathWorld
Hackathons
Computational Thinking
VIEW ALL...

Company
Events
About Wolfram
Careers
Contact

Connect
Wolfram Community
Wolfram Blog
Newsletter