Assignment Three Solutions

Jason K.C. Polák

October 23, 2013

1 Question One

> Find the gcd of $f(x) = x^4 + 3x^3 + 16x^2 + 33x + 55$ and $g(x) = x^3 + x^2 - x - 10$.

Performing long division gives

$$f(x) = (x+2)g(x) + 15(x^2 + 3x + 5).$$

Also, long division shows that $(x-2)(x^2+3x+5) = x^3 + x^2 - x - 10$ so the gcd is the monic polynomial $x^2 + 3x + 5$. By the first long division

$$\frac{1}{15}f(x) - \frac{1}{15}(x+2)g(x) = x^2 + 3x + 5.$$

Here is how to do it in Sage:

```
R.<x> = PolynomialRing(QQ)
f = x^4 + 3*x^3 + 16*x^2 + 33*x + 55
g = x^3 + x^2 - x - 10
g.xgcd(f)
>>(x^2 + 3*x + 5, -1/15*x - 2/15, 1/15)
```

2 Question Two

> Find the gcd of $f(x) = x^6 + x^4 + x + 1$ and $g(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ in $\mathbb{Z}/2[x]$ and express it as a linear combination of f and g

.

Via long division, or possibly by inspection since $\mathbb{Z}/2$ is so nice:

$$g(x) = f(x) + x^5 + x^3 + x^2$$
$$f(x) = x(x^5 + x^3 + x^2) + x^3 + x + 1$$
$$x^5 + x^3 + x^2 = x^2(x^3 + x + 1).$$

Hence the gcd is $x^3 + x + 1 = (1+x)f + xg$.

Here is how to do it in Sage:

```
R.<x> = PolynomialRing(Integers(2))
f = x^6 + x^4 + x + 1
g = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
g.xgcd(f)
>>(x^3 + x + 1, x, x + 1)
```

3 Question Three

List all the irreducible degree four polynomials in $\mathbb{Z}/2[x]$.

Any irreducible quartic $f \in \mathbb{Z}/2[x]$ has to be of the form $f(x) = x^4 + ax^3 + bx^2 + cx + 1$ where $a, b \in \mathbb{Z}/2$ since polynomials without a constant term have the irreducible factor x. However, polynomials with an even number of terms in $\mathbb{Z}/2[x]$ all have $x = 1$ as a root, so there are four remaining possibilities

- $x^4 + x + 1$,
- $x^4 + x^2 + 1$,
- $x^4 + x^3 + 1$, and
- $x^4 + x^3 + x^2 + x + 1$.

These are either irreducible or else they must be a product of quadratic factors, since a linear factor would give a root, and these have no roots. There is only one irreducible quadratic, which is $x^2 + x + 1$. Squaring this gives

$$(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1.$$

Hence the irreducible quartics are

- $x^4 + x + 1$,
- $x^4 + x^3 + 1$, and
- $x^4 + x^3 + x^2 + x + 1$.

Note that if you want to try your hand at finding the irreducible quartics in $\mathbb{Z}/p[x]$ for any prime p then there are $\frac{1}{4}p^2(p^2 - 1)$ monic ones.

4 Question Four

If $p = 4m+1$ is a prime then $(2m)!$ is a root in $\mathbb{Z}/p$ of $x^2+1 \in \mathbb{Z}/p[x]$.

Since p is a prime, Wilson's theorem gives $(4m)! \equiv -1 \pmod{p}$. Hence modulo p,

$$\begin{aligned} -1 \equiv (4m)! &\equiv 1 \cdot 2 \cdots (2m)(2m+1)(2m+2) \cdots (2m+2m) \\ &\equiv 1 \cdot 2 \cdots (2m)(-2m)(-2m+1)(-2m+2) \cdots (-2)(-1). \end{aligned}$$

Since there are an even number of terms the last line reduces to $[(2m)!]^2$, so in conclusion,

$$[(2m)!]^2 \equiv -1 \pmod{p}$$

which is exactly what we were trying to prove.

5 Question Five

> A polynomial $f \in F[x]$ for a field F has at most $d = \deg(f)$ roots. Find a counterexample to this statement without the assumption that F is a field.

There are many possibilities here, such as the examples coming out of the next question! Here is another: consider the ring $\mathbb{Z}\times\mathbb{Z}$ where addition and multiplication are given pointwise:

$$(a, b) + (a', b') = (a + a', b + b')$$
$$(a, b) \cdot (a', b') = (aa', bb').$$

Consider the polynomial $f \in (\mathbb{Z}\times\mathbb{Z})[x]$ given by $f(x) = (1, 0)x$. It is a nonzero polynomial of degree two. However, it has infinitely many roots. In fact, $(0, z)$ is a root for any $z \in \mathbb{Z}$.

The same trick can be used for any ring with *zero divisors*: recall that an element $a \in R$ is called a zero divisor if there exists a $b \in R$ such that $ab = 0$ and $b \neq 0$. If R is any ring with some $a, b \in R$, both nonzero such that $ab = 0$, then $f(x) = ax$ will have at least two solutions.

6 Question Six

> Let $n = pq$ where p and q are distinct primes. Find the best upper bound for the number of roots of polynomial in $\mathbb{Z}/n[x]$ as a function of the degree, and show that this upper bound can always be attained.

Let f be the polynomial of degree d in $\mathbb{Z}/n[x]$. If $r \in \mathbb{Z}/n$ is a root then $f(r) = 0$ in $\mathbb{Z}/n$ and consequently also when we reduce modulo p *and* modulo q via the Chinese remainder theorem. Moreover, if $s \in \mathbb{Z}/p$ is a root of f modulo p and $t \in \mathbb{Z}/q$ is a root modulo q, then there exists a unique element $r \in \mathbb{Z}/n$, necessarily a root, that reduces to s mod p and t mod q.

Since there are at most $\min(d, p)$ in $\mathbb{Z}/p$ and $\min(d, p)$ roots in $\mathbb{Z}/q$, f must have at most $R(d) = \min(d, p) \min(d, q)$ roots in $\mathbb{Z}/pq$. We claim that this is the best possible upper bound. In fact, following our above reasoning $x(x - 1) \cdots (x - d)$ shows this.

6.1 Example

Consider the ring $\mathbb{Z}/21$. Let us try and find a quartic polynomial with twelve roots. The above scheme actually allows us to find it easily: it is $f(x) = x(x - 1)(x - 2)(x - 3) =$

$x^4 - 6x^3 + 11x^2 - 6x$. Modulo 3, it has the roots, $0, 1, 2$ (one is repeated on this reduction) and modulo 7 it has the roots $0, 1, 2, 3$.

Of course now finding all the roots in $\mathbb{Z}/21$ is just an exercise in reversing the reduction modulo p in the Chinese remainder theorem. Since $\gcd(p, q) = 1$ we can write 1 as a $\mathbb{Z}$-linear combination of p and q:

$$-2 \cdot 3 + 7 = 1.$$

Recall now that if we want to find the unique element $x \in \mathbb{Z}/21$ such that $x \equiv a \pmod 3$ and $x \equiv b \pmod 7$ then we just take $a(1 + 6) + b(1 - 7) = 7a - 6b$. Doing this we find the roots:

a	b	7a - 6b
0	0	0
0	1	15
0	2	9
0	3	3
1	0	7
1	1	1
1	2	16
1	3	10
2	0	12
2	1	8
2	2	2
2	3	17

7 Question Seven

Write the nonzero powers of x in $\mathbb{Z}/2[x]/(x^3+x+1)$ and every nonzero element can be written as a power of x.

The powers are:

1. x
2. x^2
3. $x^3 = 1 + x$
4. $x^4 = x + x^2$
5. $x^5 = 1 + x + x^2$
6. $x^6 = x + x^2 + 1 + x = 1 + x^2$
7. $x^7 = x + x^3 = 1$

All of these powers have degree less than two and hence are distinct, and since all the elements of $\mathbb{Z}/2[x]/(x^3+x+1)$ are represented by a polynomial of degree at most two, these are all the elements, since each such polynomial appears in this list. (Since x^3+x+1 has no root in $\mathbb{Z}/2$ and it is cubic, it is irreducible so $\mathbb{Z}/2[x]/(x^3+x+1)$ is a field with $2^3 = 8$ elements.).

8 Question Eight

For any $g \in \mathbb{Z}/p[x]$ the degree of $f = \gcd(x^p - x, g(x))$ is exactly the number of distinct roots of g.

By Fermat's little theorem, $x^p - x$ has p distinct roots in $\mathbb{Z}/p$ and so $x - a | x^p - x$ for every $a \in \mathbb{Z}/p$. Hence $x^p - x$ is just the polynomial $x(x-1)\cdots(x-p+1)$, since they are both monic and differ by multiplication of some invertible element

Thus f is some subproduct of $x(x-1)\cdots(x-p+1)$, and $x - a|f$ if and only if a is a root of g. Since f has no repeated roots, $\deg(f)$ is the number of roots of g.

9 Question Nine

The polynomial $x^2 + 1$ has no roots in $\mathbb{Z}/p$ if $p = 4m + 3$.

We use the results of Question Eight and compute $\gcd(x^p - x, x^2 + 1)$. First,

$$(x^2+1)(x - x^3 + x^5 - x^7 + x^9 - \cdots - x^{4m-1} + x^{4m+1}) = x^{4m+3} + x.$$

In other words, $x^{4m+3} \equiv -2x \pmod{x^2+1}$. By inspection, $\gcd(x^2+1, x) = 1$, so x^2+1 has $\deg(1) = 0$ roots.

10 Question Ten

Describe a realistic algorithm to find the number of roots of a polynomial $f \in \mathbb{Z}/p[x]$.

If we use Question Eight, then the Euclidean algorithm can determine the greatest common divisor of $f(x)$ and $x^p - x$, so that the number of roots can be read off from the degree of this gcd. In order to make this computation efficient for very large p, then it is necessary to use something more than naive division, since if p is very large then dividing $f(x)$ into $x^p - x$ will take an exceptionally large number of steps (think of dividing $x^p - x$ by $x - 1$: since $x^p - x = x(x^{p-1} - 1) = x(x-1)(x^{p-2} + x^{p-3} + \cdots + 1)$. Using the naive division algorithm would result on the order of p operations. For a 30-digit prime, p operations at 10 billion operations per second would take about 32 billion millenia.)

Hence, the first step in the algorithm, $x^p - x = qf(x) + r(x)$ ought to be done a bit more efficiently. To do this, we find the remainder of x^p on division by $f(x)$. To do this we use successive squaring: computing $x^2, x^4, x^8, \dots$ modulo $f(x)$. Once $x^{2^{n-1}}$ is found modulo $f(x)$, we just square that to and then reduce.

Then writing $x^p = x^{\sum 2^k}$ where $\sum 2^k = p$ is the binary expansion of p, we just have to multiply all the powers we found above, and then reduce modulo f again. Since the total number of binary digits of p is on the order of $\log_2(p)$, this is much more efficient. For instance, a thirty digit prime has $30 \log_2(10) \approx 43.4$ so we should need at most 44 squarings.