

Contents

1	Quadratic Sieve	1
2	Exercise 11.4: factorise 1679	1
3	$a^2 - 6b^2$ is divisible by 7 means 6 is a square modulo 7	2
4	Prime Ideal $\mathfrak{p} = \langle p, \sqrt{d} - r \rangle$	2
4.1	Restriction of ϕ to \mathbb{Z} is \mathbb{F}_p	3
4.2	All Cases	3
4.3	$\left(\frac{r}{p}\right) = 1 \Rightarrow \langle p \rangle = \mathfrak{p}_1 \mathfrak{p}_2$	3

1 Quadratic Sieve

$$x^2 \equiv N \pmod{p}$$

$$x \equiv a_p \pmod{p} \text{ or } x \equiv b_p \pmod{p}$$

$$x^2 - 227179 \equiv 0 \pmod{5}$$

$$x \equiv 2, 3 \pmod{5}$$

$$(\langle 5 \rangle + 2)^2 - N = \langle 5 \rangle$$

\$ sage ch11-quadratic-sieve.sage

---	-----	-----	-----
470	-6279	-1 * 3 * 7 * 13 * 23	[1, 0, 1, 0, 1, 0, 1, 0, 0, 1]
473	-3450	-1 * 2 * 3 * 5^2 * 23	[1, 1, 1, 0, 0, 0, 0, 0, 0, 1]
477	350	2 * 5^2 * 7	[0, 1, 0, 0, 1, 0, 0, 0, 0, 0]
482	5145	3 * 5 * 7^3	[0, 0, 1, 1, 1, 0, 0, 0, 0, 0]
493	15870	2 * 3 * 5 * 23^2	[0, 1, 1, 1, 0, 0, 0, 0, 0, 0]
---	-----	-----	-----

212460² 169050² (mod 227179)
227179 = 157 * 1447

So we see 5 divides all x that are of the form $5a + 2$ or $5a + 3$.

2 Exercise 11.4: factorise 1679

We are given $(a, b) = (-1, 2), (5, 4)$ and $1679 = 41^2 - 2$.

$$\mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}/\langle 1679 \rangle$$

$$a + b\sqrt{2} \rightarrow a + 41b$$

$$N((-1, 2)) = N((5, 4)) = -7$$

$$\phi((-1, 2)) = 81 = 3^4, \quad N((5, 4)) = 169 = 13^2$$

$$(-1 + 2\sqrt{2})(5 + 4\sqrt{2}) = 11 + 6\sqrt{2}$$

$$= (3 + \sqrt{2})^2$$

$$\phi(3 + \sqrt{2}) = 44$$

$$\Rightarrow 44^2 = (3^2 13)^2 \pmod{1679}$$

```

sage: var("x")
x
sage: R.<a> = NumberField(x^2 - 2)
sage: sqrt((-1 + 2*a)*(5 + 4*a))
a + 3
sage: (3 + a)^2
6*a + 11
sage: 6*41 + 11
257
sage: Mod(44, 1679)^2 == 257^2
False
sage: Mod(44, 1679)^2
257
sage: 3^2 * 13
117
sage: Mod(44, 1679)^2 == 117^2
True

sage: gcd(1679, 117 + 44)
23
sage: gcd(1679, 117 - 44)
73
sage: 23 * 73
1679

```

3 $a^2 - 6b^2$ is divisible by 7 means 6 is a square modulo 7

1. $(c^2)^{-1} = (c^{-1})^2$ so we see the inverse of a square is also a square.
2. $a^2 - 6b^2 \equiv 0 \pmod{7} \Rightarrow a^2 b^{-2} \equiv 6 \pmod{7}$
3. $\text{kronecker}(6, 7) = -1$, so 7 cannot be a divisor of the norm.

By the same argument, we can see that 6 modulo p must be a quadratic residue.

4 Prime Ideal $\mathfrak{p} = \langle p, \sqrt{d} - r \rangle$

We saw in chapter 5 that

$$\mathbb{Z}_K/\mathfrak{p}_i \cong \mathbb{F}_p[X]/\langle \bar{g}_i(X) \rangle$$

so the quotient ring contains \mathbb{F}_p .

We know $\mathbb{Z}_K/\mathfrak{p}$ is a finite field with a cardinality measured by the norm which is a power of p . All finite fields contain a subfield \mathbb{F}_p by Cauchy. In this subfield p is the zero.

Since $p \in \mathfrak{p}$, we see that $\phi(\mathbb{Z}) = \mathbb{F}_p$, which is the restriction of $\phi|_{\mathbb{Z}}$.

1. The ideal \mathfrak{p} is a factorization of $\langle a + b\sqrt{d} \rangle$, where $N(\langle a + b\sqrt{d} \rangle) = a^2 - db^2$.
2. We assume $p|N(\langle a + b\sqrt{d} \rangle)$, which means $p \in \langle a + b\sqrt{d} \rangle \subseteq \mathfrak{p}$.
3. Consider the map ϕ which is a homomorphism.
4. We see that $\phi(a + b\sqrt{d}) = \mathfrak{p}$. Rearranging this, we get $\phi(\sqrt{d}) = -\phi(ab^{-1})$.
5. We showed in `ch9.md` (title $\mathbb{Z}_K = \mathbb{Z} + \pi\mathbb{Z}_K$) that the cosets of $\mathbb{Z}_K/\mathfrak{p}$ are of the form $a + \mathfrak{p}$ where $a \in \{0, \dots, p-1\}$.
6. Finally we have $a + b\sqrt{d} = pq + (a - pq) + b\sqrt{d}$, where $|a - pq| < p$. Then we can set $r = ab^{-1}$, and we see $\mathfrak{p} = \langle p, \sqrt{d} - r \rangle$.
7. Finally we have $a + b\sqrt{d} = b(ab^{-1} + \sqrt{d})$, and minus some multiple of p , so $r \equiv -ab^{-1} \pmod{p}$.

$$\mathfrak{p} = \langle p, \sqrt{d} - r \rangle$$

\mathfrak{p} has norm p due to its coset representation, and the right hand side also has norm p due to how we constructed it.

4.1 Restriction of ϕ to \mathbb{Z} is \mathbb{F}_p

Let a, a' be such that $a \equiv a' \pmod{p} \Rightarrow a \equiv a' \pmod{\mathfrak{p}}$ since $p \in \mathfrak{p}$.

Likewise $a \equiv a' \pmod{\mathfrak{p}} \Rightarrow \langle a - a' \rangle \subseteq \mathfrak{p}$ but $N(\mathfrak{p}) = p^k \Rightarrow N(\langle a - a' \rangle) | p^k$ so $p | a - a' \Rightarrow a \equiv a' \pmod{p}$.

So the cosets of $a + \mathfrak{p}$ with $a \in \{0, \dots, p-1\}$ are distinct.

4.2 All Cases

1. If $p > 2, \left(\frac{d}{p}\right) = 1$, or $p = 2, d \equiv 1 \pmod{8}$ then

$$\langle p \rangle = \mathfrak{p}_1 \mathfrak{p}_2$$

2. If $p > 2, p | d$, or $p = 2, d \equiv 2, 3 \pmod{4}$ then

$$\langle p \rangle = \mathfrak{p}^2$$

3. If $p > 2, \left(\frac{d}{p}\right) = -1$, or $p = 2, d \equiv 5 \pmod{8}$ then $\langle p \rangle$ is a prime ideal of \mathbb{Z}_K .

4.3 $\left(\frac{r}{p}\right) = 1 \Rightarrow \langle p \rangle = \mathfrak{p}_1 \mathfrak{p}_2$

Let $\mathfrak{p}_1 = \langle p, r + \sqrt{d} \rangle, \mathfrak{p}_2 = \langle p, r - \sqrt{d} \rangle$.

We prove first $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Suppose $\mathfrak{p}_1 = \mathfrak{p}_2$, then $2a = (r + \sqrt{d}) + (r - \sqrt{d}) \in \mathfrak{p}_1$. But $2a \in \mathbb{Z}$ so $2a \in \mathfrak{p}_1 \cap \mathbb{Z} = \langle p \rangle$. Hence $p | 2a$ but this is impossible since p is odd.

Now multiply $\mathfrak{p}_1 \mathfrak{p}_2$

$$\begin{aligned} \mathfrak{p}_1 \mathfrak{p}_2 &= \langle p, r + \sqrt{d} \rangle \langle p, r - \sqrt{d} \rangle \\ &= \langle p \rangle I \end{aligned}$$

$$I = \langle p, r + \sqrt{d}, r - \sqrt{d}, (r^2 - d)/p \rangle$$

Since $\gcd(2r, p) = 1$, there are integers x, y such that

$$xp + y(2r) = 1$$

$$\Rightarrow 1 = xp + y(2r) = xp + (r + \sqrt{d}) + (r - \sqrt{d}) \in I$$

$$I = \langle 1 \rangle$$

$$\langle p \rangle = \mathfrak{p}_1 \mathfrak{p}_2$$