Course 2316 — Sample Paper 2

Timothy Murphy

April 20, 2015

Attempt 5 questions. All carry the same mark.

1. Determine $d = \gcd(2009, 2317)$, and find integers m, n such that

$$2009m + 2317n = d.$$

Answer:

(a) *Following the Euclidean Algorithm,*

$$\begin{aligned} 2317 &= 2009 + 308, \\ 2009 &= 308 \cdot 6 + 161, \\ 308 &= 161 \cdot 2 - 14, \\ 161 &= 14 \cdot 11 + 7, \\ 14 &= 7 \cdot 2. \end{aligned}$$

It follows that

$$d = \gcd(2009, 2317) = 7.$$

(b) *Wording backwards,*

$$\begin{aligned} 7 &= 161 - 14 \cdot 11 \\ &= 161 - (161 \cdot 2 - 308) \cdot 11 \\ &= 308 \cdot 11 - 161 \cdot 21 \\ &= 308 \cdot 11 - (2009 - 308 \cdot 6) \cdot 21 \\ &= 308 \cdot 137 - 2009 \cdot 21 \\ &= (2317 - 2009) \cdot 137 - 2009 \cdot 21 \\ &= 2317 \cdot 137 - 2009 \cdot 158. \end{aligned}$$

Thus

$$2009 \cdot -158 + 2317 \cdot 137 = 7.$$

2. Find the smallest positive multiple of 2009 ending in the digits 001, or else show that there is no such multiple.

   Answer: *We are trying to solve the congruence*

   $$2009n \equiv 1 \bmod 1000,$$

   ie

   $$9n \equiv 1 \bmod 1000.$$

   Since

   $$9 \cdot 111 = 999 \equiv -1 \bmod 1000$$

   it follows that

   $$\frac{1}{9} \equiv -111 \bmod 1000.$$

   Multiplying the congruence by $1/9 \bmod 1000$*,*

   $$n \equiv -111 \bmod 1000,$$

   ie

   $$n = -111 + 1000t.$$

   Thus the smallest positive solution is

   $$n = -111 + 1000 = 889.$$

3. Define Euler's totient function $\phi(n)$, and show that if a is coprime to n then

   $$a^{\phi(n)} \equiv 1 \bmod n.$$

   Determine the smallest power of 2317 ending in the digits 001.

   Answer:

   (a) *$\phi(n)$ is the number of integers $a \in [0, n)$ coprime to n.*

(b) *Let* $(\mathbb{Z}/n)^*$ *denote the set of residues* mod n *coprime to* n.

Then $(\mathbb{Z}/n)^n$ *forms a group under multiplication* mod n, *with neutral element* $1 \bmod n$.

For if a, b *are coprime to* n *then so is* ab. *Moreover, if* a *is coprime to* n *then the map*

$$x \mapsto ax : (\mathbb{Z}/n)^* \to (\mathbb{Z}/n)^*$$

is injective, since

$$\begin{aligned} ax \equiv ay \bmod n &\implies a(x-y) \equiv 0 \bmod n \\ &\implies x - y \equiv 0 \bmod n \\ &\implies x \equiv y \bmod n. \end{aligned}$$

Hence the map is surjective, and so a *has an inverse* $b \bmod n$ *with*

$$ab \equiv 1 \bmod n.$$

It follows that $(\mathbb{Z}/n)^*$ *is a group.*

By definition, the group is of order $\phi(n)$. *It follows by Lagrange's Theorem that*

$$g^{\phi(n)} = 1$$

for all $g \in (\mathbb{Z}/n)^*$, *ie*

$$a^{\phi(n)} \equiv 1 \bmod n$$

for all a *coprime to* n.

(c) *We are trying to solve the congruence*

$$2317^n \equiv 1 \bmod 1000,$$

ie

$$317^n \equiv 1 \bmod 1000.$$

By the Chinese Remainder Theorem, this is equivalent to

$$317^n \equiv 1 \bmod 8 \textit{ and } 317^n \equiv 1 \bmod 125.$$

The first congruence reduces to

$$5^n \equiv 1 \bmod 8.$$

Since

$$5^2 \equiv 1 \bmod 8,$$

the congruence holds if and only if n is even.
The second congruence reduces to

$$67^n \equiv 1 \bmod 125.$$

Thus we have to determine the order of $\overline{67}$ in the group $(\mathbb{Z}/125)^*$. This group has order

$$\phi(125) = 5^3 - 5^2 = 100,$$

since there are just $125/5 = 25$ numbers in $[0, 125)$ divisible by 5.
It follows that the order of $67 \bmod 125$ divides 100.
Since

$$67 \equiv 2 \bmod 5$$

and the order of $2 \bmod 5$ is 4, it follows that the order of $67 \bmod 125$ is divisible by 4. Hence it is 4,20 or 100.
A computer can determine $a^n \bmod m$ very quickly, even if the numbers are large. The standard way is to express n to base 2, ie as a sum

$$n = 2^{e_1} + 2^{e_2} + 2^{e_3} + \cdots,$$

and then successively square $a \bmod m$.
But we don't have a computer. I don't know a better way to answer the question than to play with modular arithmetic.
Let us first work out the order $\bmod 25$, which we know is either 4 or 20.
We have

$$67 \equiv 17 \equiv -8 \bmod 25.$$

So

$$67^4 \equiv (-8)^4 \equiv 2^{12} \bmod 25.$$

Now if we play with computers we know that

$$2^{10} = 1024.$$

Hence

$$2^{12} = 4096 \equiv -4 \bmod 25.$$

So 67 must have order $20 \bmod 25$. Thus 67 has order 20 or 100 $\bmod 125$.

We have

$$67 = 3 \cdot 5^2 - 2^3.$$

By the binomial theorem

$$67^5 \equiv -2^{15} \bmod 5^3,$$

since the other terms in the binomial expansion will all contain 5 to at least the power 3.

It follows that

$$67^{20} \equiv 2^{60} \bmod 5^3.$$

If now 67 has order 20 then the order of 2 divides 60, and so must be 5 or 20 (since it also divides $\phi(125) = 100$*).*

The order of 2 mod 125 *is certainly not 5, since* $2^5 = 32$.

So if the order of 67 is 20 then so is the order of 2. Conversely, if the order of 2 is 20 then so is the order of 67.

Thus the problem is reduced to determining the order of 2 mod 125.

We have

$$2^{10} = 1024 \equiv 24 \bmod 125.$$

Thus

$$2^{20} \equiv 24^2 = 4 \cdot 144 \equiv 4 \cdot 19 = 76 \bmod 125.$$

We conclude that 20 has order 100, and so too has 67.

Thus the smallest power of 2317 ending in 001 is 100.

[Nb There are many ways of completing the last part of the question; I've just given the first that occurs to me, to show how one can play modular arithmetic.]

4. Explain what is meant by a *primitive root* modulo an odd prime p. and find all primitive roots mod 19.

   Answer:

   (a) *The multiplicative group* $(\mathbb{Z}/p)^*$ *is cyclic. A primitive root* mod$p$ *is a generator of this group, ie a number coprime to p of order* $(p-1) \bmod p$.

   (b) *Since* $(\mathbb{Z}/19)^*$ *has order 18, the order of any number coprime to 19 divides 18, ie the order is 1,2,3,6,9 or 18.*

   Consider 2. Evidently $2^e \not\equiv 1 \bmod 19$ *for* $e = 1, 2, 3$. *We have*

$$2^6 = 64 \equiv 7 \bmod 19,$$

and so

$$2^9 = 2^3 \cdot 2^6 \equiv 8 \bmod 7 = 56 \equiv -1 \bmod 19.$$

It follows that the order of $2 \bmod 19$ *is 18, ie 2 is a primitive root.*

Lemma. If $G = \langle g \rangle$ is a finite group of order n generated by g then g^e is a generator of G if and only if $\gcd(e, n) = 1$.

It follows that there are

$$\phi(18) = \phi(2)\phi(3^2) = 6$$

primitive roots $\bmod 19$, *namely*

$$2^e \quad (e = 1, 5, 7, 11, 13, 17).$$

Since

$$2^{18} \equiv 1 \bmod 19,$$

we can write these as

$$2^{\pm 1}, 2^{\pm 5}, 2^{\pm 7}.$$

Now

$$\begin{aligned} 2^5 &= 32 \equiv -4 \bmod 19, \\ 2^7 &= 4 \cdot 2^5 \equiv -16 \equiv 3 \bmod 19. \end{aligned}$$

Since

$$\begin{aligned} 2^{-1} &\equiv 10 \bmod 19, \\ 4^{-1} &\equiv 5 \bmod 19, \\ 3^{-1} &\equiv -6 \bmod 19 \end{aligned}$$

we see that the primitive roots $\bmod 19$ *are*

$$2, 3, 5, 10, 13, 14.$$

5. Show that if $d > 0$ is not a perfect square then Pell's equation

$$x^2 - dy^2 = 1$$

has an infinity of integer solutions.

Does the equation

$$x^2 - 5y^2 = -1$$

have an integer solution?

Answer:

(a) **Lemma.** Given $\alpha \in \mathbb{R}$ there are an infinity of approximants such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Applying this with $\alpha = \sqrt{d}$ we see that there are an infinity of $p, q \in \mathbb{Z}$ such that

$$\left|q\sqrt{d} - p\right| < \frac{1}{q}.$$

But then

$$\left|q\sqrt{d} + p\right| < 2q\sqrt{d} + \frac{1}{q}.$$

Multiplying these two inequalities,

$$\left|(q\sqrt{d} + p)(q\sqrt{d} + p)\right| = \left|p^2 - dq^2\right| < 2\sqrt{d} + \frac{1}{q^2}.$$

It follows that are an infinity of p, q such that

$$p^2 - dq^2 = \pm N,$$

for some $N < 2\sqrt{d} + 1$. (We mean either an infinity such that $p^2 - dq^2 = N$, or else an infinity such that $p^2 - dq^2 = -N$.)
Also, among this infinity of solutions there must be an infinite number such that

$$p \equiv r \bmod N, \; q \equiv s \bmod N$$

for some $r, s \in [0, N)$.
Suppose $(p, q), (P, Q)$ are two such solutions. Let

$$z = \frac{p + q\sqrt{d}}{P + Q\sqrt{d}} = x + y\sqrt{d},$$

with $x, y \in \mathbb{Q}$. Then

$$\begin{aligned} \mathcal{N}(z) &= \frac{\mathcal{N}(p + q\sqrt{d}}{\mathcal{N}(P + Q\sqrt{d}} \\ &= \frac{N}{N} \\ &= 1, \end{aligned}$$

ie

$$x^2 - dy^2 = 1.$$

We shall show that in fact

$$x, y \in \mathbb{Z}.$$

We have

$$\begin{aligned} z &= \frac{(p + q\sqrt{d})(P - Q\sqrt{d})}{P^2 - dQ^2} \\ &= \pm\frac{(p + q\sqrt{d})(P - Q\sqrt{d})}{N} \\ &= \pm\frac{(pP - qQd) + (-pQ + qP)\sqrt{d}}{N}, \\ &= \pm\frac{m + n\sqrt{d}}{N}, \end{aligned}$$

say.
Now

$$p \equiv P,\ q \equiv Q \implies n = -pQ + qP \equiv 0 \bmod N.$$

Also

$$m + n\sqrt{d} = (p + q\sqrt{d})(P - Q\sqrt{d}),$$

and so

$$\mathcal{N}(m + n\sqrt{d}) = \mathcal{N}(p + q\sqrt{d})\,\mathcal{N}(P - Q\sqrt{d})$$

ie

$$m^2 - dn^2 = N^2.$$

Hence

$$N \mid n \implies N \mid m.$$

Thus

$$x = \frac{m}{N} \in \mathbb{Z},\ y = \frac{n}{N} \in \mathbb{Z},$$

giving an integral solution of

$$x^2 - dy^2 = 1.$$

(b) *The equation*

$$x^2 - 5y^2 = -1$$

has the obvious solution

$$2^2 - 5 \cdot 1^2 = -1.$$

6. Express each of the following numbers as a sum of two squares, or else show that the number cannot be expressed in this way:

$$23,\ 101,\ 2009,\ 2010,\ 2317.$$

Answer: Lemma. The integer $n > 0$ is expressible as a sum of 2 squares if and only if each prime $p \equiv 3 \bmod 4$ divides n to an even power.

(a) *23 is prime, and* $23 \equiv 3 \bmod 4$. *Hence it is not expressible as a sum of 2 squares.*

(b) *101 is prime, and* $101 \equiv 1 \bmod 4$. *Hence it is expressible as a sum of 2 squares; and trivially*

$$101 = 10^2 + 1^2.$$

(c) *We see that*

$$2009 = 7 \cdot 287 = 7^2 \cdot 41.$$

Since each prime $\equiv 3 \bmod 4$ *divides 2009 to an even power, it must be expressible as the sum of two squares:*

$$2009 = a^2 + b^2.$$

Moreover

$$7 \mid a, b;$$

for if 7 divides one it must divide other, and if 7 divides neither then

$$a^2, b^2 \equiv 1, 2 \text{ or } 4 \bmod 7,$$

and these cannot add to $0 \bmod 7$.

[This also follows from the fact that ring Γ *of gaussian integers is a unique factorisation domain, in which 7 is a prime, so that*

$$\begin{aligned} 7 \mid a^2 + b^2 = (a+ib)(a-ib) &\implies 7 \mid (a+ib) \text{ or } 7 \mid (a-ib) \\ &\implies 7 \mid a, b. \end{aligned}$$

In fact this argument shows that if $p \equiv 3 \bmod 4$ *and* p^{2e} *exactly divides* n*, ie* $p^{2e} \mid n$ *but* $p^{2e+1} \nmid n$*, then*

$$n = a^2 + b^2 \implies p^e \mid a, b.\,]$$

Thus

$$a = 7c,\ b = 7d,$$

with

$$c^2 + d^2 = 41.$$

Evidently

$$41 = 5^2 + 4^2,$$

and so

$$2009 = 35^2 + 28^2.$$

(d) *Since the digits of 2010 add up to 3, it is divisible by 3 but not by 9. Hence 3 divides 2010 to an odd power, and so 2010 is not expressible as a sum of two squares.*

(e) *Since*

$$2317 = 7 \cdot 331,$$

and

$$7 \nmid 331,$$

7 occurs to the first power, and so 2317 is not expressible as a sum of two squares.

7. Show that if the prime p satisfies $p \equiv 3 \bmod 4$ then

$$M = 2^p - 1$$

is prime if and only if

$$\phi^{2^p} \equiv -1 \bmod M,$$

where $\phi = (\sqrt{5} + 1)/2$.

Answer: *Suppose* M *is prime. Then*

$$\phi^M = \frac{(\sqrt{5} + 1)^M}{2^M}.$$

Expanding by the binomial theorem, and noting that all the binomial coefficients except the first and last are divisible by M,

$$\begin{aligned}
\phi^M &= \frac{(\sqrt{5}+1)^M}{2^M} \\
&\equiv \frac{\sqrt{5}^M + 1}{2^M} \bmod M \\
&\equiv \frac{5^{(M-1)/2}\sqrt{5}+1}{2^M} \bmod M
\end{aligned}$$

By Fermat's Little Theorem,

$$2^M \equiv 2 \bmod M.$$

Also, by Eisenstein's criterion,

$$5^{(M-1)/2} \equiv \left(\frac{5}{M}\right) \bmod M.$$

By Gauss' Quadratic Reciprocity Law,

$$\left(\frac{5}{M}\right) = \left(\frac{M}{5}\right).$$

But since $p \equiv 3 \bmod 4$, *and* $2^4 \equiv 1 \bmod 5$,

$$2^p \equiv 2^3 \equiv 3 \bmod 5,$$

and so

$$M = 2^p - 1 \equiv 2 \bmod 5.$$

Hence

$$5^{(M-1)/2} \equiv -1 \bmod M.$$

Thus

$$\begin{aligned}
\phi^M &\equiv \frac{-\sqrt{5}+1}{2} \bmod M \\
&= -\phi^{-1}.
\end{aligned}$$

It follows that

$$\phi^{2^p} = \phi^{M+1} \equiv (-\phi^{-1})\phi = -1 \bmod M.$$

Conversely, suppose that this is the case, and suppose M is composite. Since

$$M \equiv 2 \bmod 5,$$

M has a prime factor

$$P \equiv \pm 2 \bmod 5;$$

and

$$\phi^{2^p} \equiv -1 \bmod P.$$

Now P does not split in the ring $\mathbb{Z}[\phi]$ (the ring of integers in the field $\mathbb{Q}(\sqrt{5})$). For if it did, say

$$(a + b\phi) \mid P,$$

where $a, b \in \mathbb{Z}$. Then

$$\mathcal{N}(a + b\phi) = (a + b\phi)(a + b\bar{\phi}) = a^2 + ab - b^2$$

divides $\mathcal{N}(P) = P^2$, and in particular

$$a^2 + ab - b^2 \equiv 0 \bmod P.$$

Multiplying by 4,

$$(2a - b)^2 - 5b^2 \equiv 0 \bmod P.$$

It follows that 5 is a quadratic residue mod P. *But*

$$\left(\frac{5}{P}\right) = \left(\frac{P}{5}\right) = -1,$$

since $P \equiv \pm 2 \bmod 5$.

Hence P remains prime in the ring $\mathbb{Z}[\phi]$, and so

$$F = \mathbb{Z}[\phi]/(P)$$

is a field, containing P^2 elements (represented by $a + b\phi$, where $a, b \in [0, P)$).

Thus

$$F^* = (\mathbb{Z}[\phi]/P)^*$$

is a group of order $P^2 - 1$.

It follows by Lagrange's Theorem that the order of $\phi \bmod P$ divides $P^2 - 1$.

On the other hand, it follows from

$$\phi^{2^p} \equiv -1 \bmod P$$

that the order of $\phi \bmod P$ *is* 2^{p+1}.

(For

$$\phi^{2^{p+1}} = (\phi^{2^p})^2 \equiv 1 \bmod P,$$

so the order divides 2^{p+1}*, but does not divide* 2^p*.)*

Hence

$$2^{p+1} | P^2 - 1.$$

But that is impossible, since

$$P^2 - 1 < M^2 < 2^{p+1}.$$

We conclude that M *is prime.*

8. Show that the ring $\mathbb{Z}[\sqrt{2}]$ formed by the numbers $m + n\sqrt{2}$ $(m, n \in \mathbb{Z})$ is a Unique Factorisation Domain, and determine the units and primes in this domain.

Answer:

(a) **Lemma.** The norm

$$\mathcal{N}(x + y\sqrt{2}) = x^2 - 2y^2 \quad (x, y \in \mathbb{Q})$$

is multiplicative, ie if $z, w \in \mathbb{Q}[\sqrt{2}]$ then

$$\mathcal{N}(wz) = \mathcal{N}(w)\,\mathcal{N}(z).$$

Now suppose $u, v \in \mathbb{Z}[\sqrt{2}]$*. Let*

$$\frac{u}{v} = x + y\sqrt{2},$$

with $x, y \in \mathbb{Q}$*. Choose* m, n *so that*

$$|x - m|\,, |y - n| \leq \frac{1}{2}.$$

Let

$$q = m + n\sqrt{2}.$$

Then

$$\frac{u}{v} - q = (x-m) + (y-n)\sqrt{2}.$$

Hence

$$\mathcal{N}\left(\frac{u}{v} - q\right) = (x-m)^2 - 2(y-n)^2 \in [-1/2, 1/4].$$

In particular

$$\left|\mathcal{N}\left(\frac{u}{v} - q\right)\right| < 1,$$

and so

$$|\mathcal{N}(u - qv)| < |\mathcal{N}(v)|,$$

ie

$$u = qv + r,$$

with

$$|\mathcal{N}(r)| < |\mathcal{N}(v)|.$$

This allows us to compute $\gcd(u,v)$ *for any 2 elements* $u, v \in \mathbb{Z}[\sqrt{2}]$*, using the Euclidean Algorithm:*

$$\begin{aligned}
u &= q_1 v + r_1, \\
v &= q_2 r_1 + r_2, \\
r_1 &= q_3 r_2 + r_3, \\
&\cdots \\
r_{m-1} &= q_{m+1} r_m,
\end{aligned}$$

with

$$|\mathcal{N}(r_1)| > |\mathcal{N}(r_2)| > |\mathcal{N}(r_3)| > \cdots.$$

The process must end, since the $|\mathcal{N}(r)|$ *are decreasing positive integers; and we have*

$$\gcd(u,v) = r_m.$$

Also, working backwards, we can find $x, y \in \mathbb{Z}[\sqrt{2}]$ *such that*

$$ux + vy = \gcd(u,v).$$

From this, we deduce the analogue of Euclid's Lemma: If $\pi \in \mathbb{Z}[\sqrt{2}]$ *is irreducible then*

$$\pi \mid uv \implies \pi \mid u \text{ or } \pi \mid v,$$

for $u, v \in \mathbb{Z}[\sqrt{2}]$.

Lemma. The element $\epsilon \in \mathbb{Z}[\sqrt{2}]$ is a unit, ie is invertible in this ring, if and only if

$$\mathcal{N}(\epsilon) = \pm 1.$$

Any non-unit $u \in \mathbb{Z}[\sqrt{2}]$ *is expressible as a product of irreducibles. For*

$$u = vw \implies |\mathcal{N}(u)| = |\mathcal{N}(v)|\,|\mathcal{N}(w)|$$

with

$$|\mathcal{N}(v)|\,, |\mathcal{N}(w)| < |\mathcal{N}(u)|\,,$$

so the factorisation must end after a finite number of divisions.

Finally, it follows easily from Euclid's Lemma that the factorisation is unique, up to order and multiplication by units.

(b) From the Lemma above, $u = m + n\sqrt{2}$ *is a unit if and only if*

$$m^2 - 2n^2 = \pm 1.$$

One solution to this is

$$1^2 - 2 \cdot 1^2 = -1,$$

giving the unit

$$\eta = 1 + \sqrt{2}.$$

In fact the units consist of the numbers

$$\pm \eta^n,$$

where $n \in \mathbb{Z}$. *For suppose* ϵ *is a unit* $\neq \pm 1$. *Then the 4 units*

$$\pm\epsilon, \pm\epsilon^{-1}$$

lie in the 4 regions $(-\infty, -1), (-1, 0), (0, 1), (1, \infty)$.

We may suppose therefore that $\epsilon > 1$. *Since* $\eta > 1$, *we can find* $n \geq 0$ *such that*

$$\eta^n \leq \epsilon < \eta^{n+1}.$$

Let

$$\theta = \eta^{-n}\epsilon.$$

Then

$$1 \leq \theta < \eta.$$

Suppose

$$\theta = m + n\sqrt{2}.$$

Then

$$\mathcal{N}(\theta) = (m + n\sqrt{2})(m - n\sqrt{2}) = \pm 1.$$

It follows that

$$m - n\sqrt{2} \in [-1, 1].$$

Hence, by addition,

$$0 \leq 2m < \eta + 1 = 2 + \sqrt{2} < 4,$$

ie

$$m = 0 \text{ or } 1.$$

It follows that

$$\theta = 1,$$

and so the primes are just the numbers

$$\pm\eta^n \quad (n \in \mathbb{Z}).$$

(c) *Suppose*

$$\pi = m + n\sqrt{2}$$

is a prime in $\mathbb{Z}[\sqrt{2}]$, *ie a non-unit irreducible.*
Let

$$\mathcal{N}(\pi) = \pm p_1 \cdots p_r.$$

Then since there is unique factorisation,

$$\pi \mid p$$

for some rational prime $p = p_i$.
Suppose

$$p = \pi\sigma.$$

Then

$$\mathcal{N}(\pi)\mathcal{N}(\sigma) = \mathcal{N}(p) = p^2.$$

Thus either

$$N(\sigma) = \pm 1,$$

in which case σ *is a unit, and* p *remains a prime in* $\mathbb{Z}[\sqrt{2}]$, *or else*

$$\mathcal{N}(\pi) = \mathcal{N}(\sigma) = \pm p.$$

In the second case,

$$\mathcal{N}(\pi) = m^2 - 2n^2 \equiv 0 \bmod p,$$

and so 2 is a quadratic residue mod p. *But we know that if p is an odd prime then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8 \end{cases}$$

Thus p remains a prime if $p \equiv \pm 3 \bmod 8$.
If $p \equiv \pm 1 \bmod 8$ then 2 is a quadratic residue, so

$$2 \equiv a^2 \bmod p,$$

for some a, ie

$$p | a^2 - 2 = (a - \sqrt{2})(a + \sqrt{2}).$$

If p remains a prime $\mathbb{Z}[\sqrt{2}]$ then (since there is unique factorisation)

$$p \mid a - \sqrt{2} \text{ or } p \mid a + \sqrt{2},$$

either of which implies that $p \mid 1$, which is absurd.
Hence p splits in $\mathbb{Z}[\sqrt{2}]$ if $p \equiv \pm 1 \bmod 8$. Also

$$\pi \mid p \implies \mathcal{N}(\pi) = \pm p,$$

so p splits into two prime factors, π and $\bar{\pi}$ (or the associated prime, $-\bar{\pi}$.
Could π and $\bar{\pi}$ be associated, ie

$$\bar{\pi} = \epsilon\pi?$$

In that case

$$p \mid \pi^2 = (m + n\sqrt{2})^2 = (m^2 + 2n^2) + 2mn\sqrt{2}.$$

It follows that

$$p \mid m^2 + 2n^2, \; p \mid 2mn.$$

Since p is odd, this implies that

$$p \mid m, n \implies p \mid \pi,$$

which is absurd.

Finally,

$$2 = (\sqrt{2})^2,$$

ie 2 splits into two equal primes (or ramifies).

In summary: 2 splits into two equal primes in $\mathbb{Z}[\sqrt{2}]$*, while the rational primes* $p \equiv \pm 3 \bmod 8$ *remain prime, and the rational primes* $p \equiv \pm 1 \bmod 8$ *split into 2 distinct primes. Moreover these give all the primes in* $\mathbb{Z}[\sqrt{2}]$*.*