


Solutions to HW2

1. (a) $(x, y) = (3, 16)$ is a solution. The third continued fraction convergent to $\sqrt{29}$ is $\frac{16}{3}$.

   (b) There is no integer solution, since there are no solutions mod 4. This follows from the fact that all integers satisfy $x^2 \equiv 0$ or $1 \mod 4$. For all integers x, y, we have $29x^2 - y^2 \equiv 0, 1$ or $3 \mod 4$, whereas $10 \equiv 2 \mod 4$.

   (c) $(x, y) = (13, 70)$ is a solution. The 5th continued fraction convergent to $\sqrt{29}$ is $\frac{70}{13}$.

   (d) There is no integer solution, since there are no solutions mod 3.

   (e) $(x, y) = (18, 97)$ is a solution.

   (f) $(x, y) = (1, 7)$ is a solution. The first continued fraction convergent to $\sqrt{61}$ is $7 = \frac{7}{1}$.

   (g) There is no integer solution, since there are no solutions mod 4. Compare with (b).

   (h) $(x, y) = (722, 5639)$ is a solution. The 10th continued fraction convergent to $\sqrt{61}$ is $\frac{5639}{722}$.

   (i) There is no integer solution, since there are no solutions mod 16 (or mod 61). To reach this conclusion, assuming you have looked for solutions mod 8, you will recall that every integer satisfies $x^2 \equiv 0, 1$ or $4 \mod 8$; so every solution must have x, y even; but then $(x, y) = (2k, 2\ell)$ gives an integer solution of $61k^2 - \ell^2 = 6$, and this has no solutions mod 4.

   (j) $(x, y) = (3805, 29718)$ is a solution. The 11th continued fraction convergent to $\sqrt{61}$ is $\frac{29718}{3805}$.

Question #1 should spur you to ask whether there is any better way to look for integer solutions (and noncongruence conditions) than using computer searches, and looking for a violation of congruence conditions. As mentioned very early in the semester, *there is no single algorithm that can determine in every case whether or not a given Diophantine equation has an integer solution.* The equations in #1 were carefully chosen to be within the realm of techniques you have currently available (including computer search in some cases) while illustrating the range of difficulties that may arise even with innocent-looking Diophantine equations.

2. See attached Mathematica worksheet.

#2. (a) We check that p is prime:

In[1]:=
```
p=9080706050401
PrimeQ[p]
```

Out[1]= 9 080 706 050 401

True

(b) We solve to obtain $b = 6\,041\,539\,438\,765$:

In[9]:=
```
b=Mod[56789*PowerMod[1234,-1,p],p]; Print["b=",b]
```

b=6 041 539 438 765

Check:

In[4]:=
```
Mod[1234*b,p]
```

Out[4]= 56 789

(c)

In[10]:=
```
c=PowerMod[123456789,9876543210,p]; Print["c=",c]
```

c=6 241 023 484 774

(d)

In[11]:=
```
k=ModularInverse[263,p-1]; Print["k=",k]
x=PowerMod[1975712412050,k,p]; Print["x=",x]
```

k=8 113 938 866 327

x=31 415 926 535

Check:

In[8]:=
```
PowerMod[x,263,p]
```

Out[8]= 1 975 712 412 050

3. (a) There are exactly 12 integer solutions $(\pm 20, 0), (0, \pm 20), (\pm 16, \pm 12), (\pm 12, \pm 16)$. Using the method of theta series described in class, let $\theta(t) = 1 + 2t + 2t^4 + 2t^9 + 2t^{16} + 2t^{25} + \cdots$. In Mathematica we expand $\theta(t)^2 = 1 + 4t + 4t^2 + \cdots + 12t^{400} + \cdots$ and read off the coefficient of t^{400}, which is 12.

   (c) There are exactly 30 integer solutions, since $400 = 2^4 \cdot 5^2$ has exactly 30 divisors $\pm 2^i 5^j$ for $i \in \{0, 1, 2, 3, 4\}$, $j \in \{0, 1, 2\}$, To obtain the 30 solutions, let x range over the 30 divisors of 400, i.e. $x \in \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 8, \pm 10, \pm 16, \pm 20, \pm 25, \pm 40, \pm 50, \pm 80, \pm 100, \pm 200, \pm 400\}$; and in each case, take $y = \frac{400}{x}$.

   (b) There are exactly 18 solutions. We require $(x+y)(x-y) = 400$. This is actually similar to (c) since we are solving $uv = 100$ where $u = \frac{1}{2}(x+y)$ and $v = \frac{1}{2}(x-y)$ where $u, v \in \mathbb{Z}$. Of course $x+y$ and $x-y$ have the same parity, and they cannot both be odd, so they must both be even; so $u = \frac{1}{2}(x+y)$ and $v = \frac{1}{2}(x-y)$ are integers. The problem is therefore equivalent to requiring integer solutions of $uv = 100$. So the problem is very similar to (b). Since $100 = 2^2 5^2$ has exactly 18 divisors $\pm 2^i 5^j$ where $i, j \in \{0, 1, 2\}$, the original problem also has 18 integer solutions. Take $u \in \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20, \pm 25, \pm 50, \pm 100\}$ and let $v = \frac{100}{u}$, $x = u+v$, $y = u-v$ to get the eighteen solutions $(x, y) \in \{(\pm 20, 0), (\pm 25, \pm 15), (\pm 29, \pm 21), (\pm 52, \pm 48), (\pm 101, \pm 99)\}$.

The *norm* of an element $z = a+bi \in \mathbb{Z}[i]$, defined by $N(z) = z\overline{z} = |z|^2 = a^2+b^2$, satisfies $N(zw) = N(z)N(w)$. It is clear that the only elements of $\mathbb{Z}[i]$ of norm 1 are $\pm 1, \pm i$; and we show that these are exactly the units of $\mathbb{Z}[i]$. In one direction this is clear: If z is a unit then $zw = 1$ for some $z, w \in \mathbb{Z}[i]$, so $N(z)N(w) = N(zw) = N(1) = 1$ where $N(z), N(w)$ are non-negative integers, so $N(z) = N(w) = 1$, which forces $z, w \in \{\pm 1, \pm i\}$. Conversely, if $N(z) = 1$, then $z\overline{z} = N(z) = 1$ so $\overline{z}$ is the inverse of z, and so z is a unit.

Note that the norm of an element $z \in \mathbb{Z}[i]$ has the form $N(z) = a^2+b^2 \equiv 0$, 1 or 2 mod 4.

4. (a) Since $1009 = 15^2+28^2 = (15+28i)(15-28i)$ where neither of the factors $15 \pm 28i$ is a unit, 1009 is reducible in $\mathbb{Z}[i]$.

   (b) If $2003 = zw$ where $z, w \in \mathbb{Z}[i]$, then $2003^2 = N(2003) = N(z)N(w)$ where $N(z)$ and $N(w)$ are positive integers. But we cannot have $N(z)=N(w)=2003$ since $2003 \equiv 3 \mod 4$. So one of $N(z), N(w)$ is 2003^2, and the other is 1. It follows that one of the factors z, w is a unit; so 2003 is irreducible in $\mathbb{Z}[i]$.