SOLUTIONS TO FINAL

1. (15 points) Note that $17^2 + 25^2 + 33^2 = 2003$. Prove that 2003 can be written as the sum of three rational squares in arithmetic progression in infinitely many ways. What about 2004?

   An arithmetic progression has the form $x-y$, x, $x+y$. Since $(x-y)^2+x^2+(x+y)^2 = 3x^2 + 2y^2$, it suffices to show that

   $$3x^2 + 2y^2 = 2003$$

   has infinitely many solutions. Since it has at least one, by the method of sweeping lines it has infinitely many.

   Consider the equation

   $$3x^2 + 2y^2 = 2004z^2.$$

   Reducing modulo 3 we see that $y \equiv 0 \mod 3$. Replace y by $3w$. Dividing the equation by 3, we arrive at the equation

   $$x^2 + 6w^2 = 668z^2.$$

   Reducing modulo 3 again we find that $x^2 = 2z^2 \mod 3$. The only solution to this equation is $x \equiv z \equiv 0 \mod 3$. Thus 3 divides x, y and z, and thus by the method of infinite descent, we see that the equation $3x^2 + 2y^2 = 2004z^2$ has no non-trivial solutions. Thus 2004 cannot be written as the sum of three squares in arithemetic progression.

2. (15 points) Let ℓ be prime, and let

   $$f(x) = (x^{\ell^n} - 1)/(x^{\ell^{n-1}} - 1) = x^{\ell^{n-1}(\ell-1)} + \cdots + x^{\ell^{n-1}} + 1.$$

   (a) Let $p \neq \ell$ be prime, and suppose that $f(x) \equiv 0 \mod p$ has a solution. Show there exists an element modulo p of *exact* order ℓ^n.

   (b) Show that if $\mathbb{Z}/p\mathbb{Z}$ has an element of exact order ℓ^n, then $p \equiv 1 \mod \ell^n$.

   (c) Prove that there exist infinitely many primes of the form $1 \mod \ell^n$.

   Suppose that $f(x) \equiv 0 \mod p$. Then $(x^{\ell^{n-1}}-1)f(x) = x^{\ell^n} - 1 \equiv 0 \mod p$, and x has order dividing ℓ^n. It suffices to show that x does not have order ℓ^{n-1}. Yet if $x^{\ell^{n-1}} \equiv 1 \mod p$, Then $f(x) \equiv 1 + 1 + \cdots + 1 \equiv \ell \mod p$. Since $\ell \neq p$, this is impossible.

The exact order of any element modulo p divides $p-1$. Thus ℓ^n divides $p-1$.

Suppose there are finitely many primes of the form $1 \mod \ell^n$. Then we can enumerate them as $p_1, p_2, \ldots p_k$ (possibly $k=0$). Let $N = p_1 p_2 \ldots p_k \ell$. Since $N \geq \ell \geq 2$, we see that $f(N) \geq 2$ has at least one non-trivial factor q. Since $f(N) \equiv 1 \mod N$, q is neither ℓ nor p_i for some i. Thus from part (a) we infer that $q \equiv 1 \mod \ell^n$, contradicting our assumption on primes of this form. Thus we are done.

3. (20 points) Let k be an odd integer, and suppose the equation $2x^2 + y^2 = kz^2$ has a non-trivial solution modulo n for all n. Prove that $k > 0$, and that there exists a rational solution to $2X^2 + Y^2 = k$.

   We may assume that k is squarefree. Let $k = \pm p_1 p_2 \cdots p_n$. Reducing the equation modulo p_i for any i we see that

   $$\left(\frac{-2}{p_i}\right) = 1.$$

   This quadratic symbol equals 1 if and only if $p_i \equiv 1, 3 \mod 8$. The product of any number of primes of the form 1 and 3 mod 8 is again of the form 1 or 3 mod 8. Thus $|k| = p_1 p_2 \cdots p_n \equiv 1, 3 \mod 8$. Let us now consider the original equation modulo 8. If y is even, then kz^2 is even, z is even and then x is even. Thus we may assume that y is odd. In particular, $2x^2 + y^2 \equiv 1, 3 \mod 8$. Thus z is odd, and $k \equiv 1, 3 \mod 8$. Yet we have already seen that $|k| \equiv 1, 3 \mod 8$. Thus $k = |k|$ is positive. If k is positive then the equation clearly has a solution over the real numbers, and we conclude (substituting $X = x/z$ and $Y = y/z$) by the Hasse–Minkowski theorem that $2X^2 + Y^2 = k$ has a non-trivial solution in rational numbers.

4. (15 points) Let $x_0 = 3$, and let $x_n = 3^{x_{n-1}}$ (So $x_1 = 27$, $x_2 = 7625597484987, \ldots$). Prove that the sequence x_i is eventually constant modulo n, for any integer n. Hint: prove that if $a \equiv b \mod \varphi(n)$, and a and b are sufficiently large, then $3^a \equiv 3^b \mod n$.

   First we prove the hint. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Then $\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_k^{a_k})$. In particular, $a \equiv b \mod \varphi(p_i^{a_i})$ for all i. Thus by the Chinese remainder theorem, it suffices to prove the hint for prime powers, since $a \equiv b \mod p_i^{a_i}$ for all i implies that $a \equiv b \mod n$. If $n = 3^k$, then the result is trivially true if $a, b \geq k$. Suppose that $n = p^k$ with $p \neq 3$. Since $(3, p) = 1$, by Euler's theorem $3^{\varphi(n)} \equiv 1 \mod n$. If $a \geq b$, then $a - b$ is divisible by $\varphi(n)$ by assumption and so $3^{a-b} \equiv 1 \mod n$, and thus $3^a \equiv 3^b \mod n$. This proves the lemma.

   We now return to the original problem, that we prove by induction. The result is trivial for $n = 1$. Assume the result is true for all $k < n$. Then in particular, it is true for $k = \varphi(n)$. Thus for sufficiently large i,

   $$x_i \equiv x_{i+1} \equiv \ldots \equiv x_{i+k} \mod \varphi(n)$$

Since the x_i are increasing, by the Hint proved above we infer that for sufficiently large i,

$$3^{x_i} \equiv 3^{x_{i+1}} \equiv \ldots \equiv 3^{x_{i+k}} \mod n.$$

Equivalently, $x_{i+1} \equiv x_{i+2} \equiv \ldots \equiv x_{i+k+1} \mod n$, and the sequence x_i becomes constant modulo n. This proves the induction step, and we are done.

5. (15 points) The ring $\mathbb{Z}[\sqrt{-13}]$.

   (a) Prove that $x^2 + 13y^2$ and $2x^2 + 2xy + 7y^2$ are the only reduced binary quadratic forms of discriminant -52.

   (b) Prove that a prime p can be written in the form $p = x^2 + 13y^2$ with x, y integers if and only if

$$\left(\frac{-13}{p}\right) = 1, \qquad p \equiv 1 \mod 4.$$

Consider a reduced form $ax^2 + bxy + cy^2$ of discriminant -52. Thus a, b and c satisfy with $b^2 - 4ac = -52$. Clearly $2|b$. Since $a \geq |b|$ and $c \geq |b|$, we note that $-3b^2 \geq -52$, and thus

$$|b| \leq \lfloor \sqrt{52/3} \rfloor = \lfloor 4.16333\ldots \rfloor = 4.$$

If $b = 0$ then $ac = 13$, which, since $a \leq b$, implies that $a = 1$ and $c = 13$. If $|b| = 2$, then $ac = 14$. Since $2 \leq a \leq c$, we must have $a = 2$ and $c = 7$. Since $|b| = a$, we may insist the sign of b is positive. If $|b| = 4$, then $ac = 17$, but this is not possible if $4 \leq a \leq c$. Thus $x^2 + 13y^2$ and $2x^2 + 2xy + 7y^2$ are the only reduced forms.

It is easy to see that any prime of the form $p = x^2 + 13y^2$ must satisfy the conditions given. Now let us take an odd prime p of that form. Since -13 is a quadratic residue, p factors into 2 primes $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ in $R = \mathbb{Z}[\sqrt{-13}]$. Moreover, the binary quadratic form associated to $\mathfrak{p}$ represents p. Thus any prime for which -13 is a quadratic residue can be written in terms of *some* reduced binary quadratic form of discrmininant -52 (For another arugment that any quadratic residue can be represented by at least one form, see Davenport, pg.136–137). If $p \equiv 1 \mod 4$, then a simple check modulo 4 shows that it *cannot* be written in the form $2x^2 + 2xy + 7y^2$. Thus it must be of the form $x^2 + 13y^2$.

6. (5 points) Using `pari` or otherwise, calculate the sum

$$\frac{1}{\pi^{12}} \sum_{k=1}^{1000} \frac{1}{k^{12}}$$

to high accuracy. By considering the continued fraction of this number, give a conjectural formula for the exact value of

$$\sum_{k=1}^{\infty} \frac{1}{k^{12}}.$$

One finds (to about 40 decimal places) that

$$\frac{1}{\pi^{12}}\sum_{k=1}^{1000}\frac{1}{k^{12}} = 0.000010822021404031986042568053150063731096 13\ldots$$

The continued fraction expansion of this number is

$$[924041, 1, 3, 1, 2, 2, 1, 13, 1, 2.5075075\ldots \times 10^{22}]$$

thus a reasonable guess is that the infinite sum is equal to

$$\pi^{12}[924041, 1, 3, 1, 2, 2, 1, 13, 1] = \frac{691\pi^{12}}{638512875}.$$

This is indeed the correct answer.

7. (15 points) Pell's equation.

   (a) Find the continued fraction expansion of $\sqrt{67}$.

   (b) Find the three smallest *positive* integer solutions to $x^2 - 67y^2 = 1$.

   (c) Show that if (x_{100}, y_{100}) is the 100th smallest *positive* integer solution to $x^2 - 67y^2$ then x_{100} has 499 digits.

   One finds that

$$\sqrt{67} = [8, \overline{5, 2, 1, 1, 7, 1, 1, 2, 5, 16}].$$

   Calculating the first few partial fraction convergents, we find the smallest non-trivial solution to $x^2 - 67y^2 = 1$ is $(x_1, y_1) = (48842, 5967)$. Thus the general solution is (x_n, y_n), where

$$x_n + y_n\sqrt{67} = (48842 + 5967\sqrt{67})^n.$$

   From this we find $(x_2, y_2) = (4771081927, 582880428)$, and

$$(x_3, y_3) = (466058366908226, 56938091722785).$$

   To estimate x_n, note that by taking conjugates, we find that

$$2x_n = (x_n + \sqrt{67}y_n) + (x_n - \sqrt{67}y_n) = (48842 + 5967\sqrt{67})^n + (48842 - 5967\sqrt{67})^n.$$

   We see that $(48842 - 5967\sqrt{67}) = 0.00001023\ldots$ so the 100th power of this is very small. Thus we need the number of digits of

$$\frac{1}{2}\cdot(48842 + 5967\sqrt{67})^{100}.$$

   Taking logs (to this base 10), we find that

$$100\log_{10}(48842 + 5967\sqrt{67}) - \log_{10}(2) \simeq 498.681.$$

   Thus 499 digits are required for x_{100}.