18.782 PROBLEM SET 1
SOLUTIONS

1. Rational points on circles.
(a) No. This will follow from part (b) and the observation that 2019 cannot be a sum of two integer squares since, for example, we have $2019 \equiv 3 \mod 4$ and a sum of two integer squares must be $\equiv 0, 1 \mod 4$.

(b) The “if” direction is clear, so we shall prove the “only if” direction. We begin by recalling the following elementary fact about arithmetic in $\mathbb{Z}[i]$: if $p \in \mathbb{Z}$ is a prime number, then either $p$ remains a prime in $\mathbb{Z}[i]$ or there exists a prime $\alpha \in \mathbb{Z}[i]$ such that $p = \alpha \bar{\alpha} = N(\alpha)$. Indeed, if $\alpha$ is a prime divisor of $p$ in $\mathbb{Z}[i]$ and $p = \alpha \beta$ with $\beta \in \mathbb{Z}[i]$, then $N(\alpha)$ divides $N(p) = p^2$ so either $N(\alpha) = p$ or $N(\alpha) = p^2$; in the latter case, $N(\beta) = 1$ so $\beta$ is a unit in $\mathbb{Z}[i]$, showing $p = \alpha \beta$ is prime in $\mathbb{Z}[i]$.

Suppose now that $x^2 + y^2 = k$ has a rational solution, say $(x, y) = (a/c, b/c)$ for some $a, b, c \in \mathbb{Z}$ with $\gcd(a, b, c) = 1$ and $c > 0$. In particular, we have

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

The case $k \leq 0$ is obvious, so let us assume $k \geq 1$. If $c = 1$ we are done, so suppose that $p$ is a prime number dividing $c$. Let $\alpha = a + bi$ so $kc^2 = N(\alpha)$. Let $\alpha = \beta_1 \cdots \beta_m$ be a prime factorization of $\alpha$ in $\mathbb{Z}[i]$. Then

$$kc^2 = N(\alpha) = N(\beta_1) \cdots N(\beta_m).$$

Since $p^2$ divides $kc^2$, we may assume that $p$ divides $N(\beta_1)$ up to relabeling $\beta_i$’s. If $N(\beta_1) = p^2$, then $N(\beta_2 \cdots \beta_m) = k(c/p)^2$ is a sum of two squares. On the other hand, if $N(\beta_2) = p$ then $\beta_1$ must divide $kc^2/p = N(\beta_2) \cdots N(\beta_m)$ in $\mathbb{Z}[i]$ since $\beta_1$ divides $p$. Without loss of generality we may assume $\beta_1$ is equal to $\beta_2$ or $\beta_2$ up to units, so $N(\beta_2) = p$. Then $N(\beta_3 \cdots \beta_m) = k(c/p)^2$ is a sum of two squares. Arguing by induction on the number of prime divisors of $c$, we conclude that $x^2 + y^2 = k$ must have an integral solution, as desired.

2. Rational parametrizations.
(a) First note that $(3,0) \in C_1(\mathbb{Q})$. Given a line through $(3,0)$ of slope $t \in \mathbb{Q}$,

$$y = t(x - 3)$$

so at an intersection point of this line with the curve $x^2 - 5y^2 = 9$ we have

$$x^2 - 5t^2(x - 3)^2 = 9 \implies (x - 3)(x + 3 - 5t^2(x - 3)) = 0$$

showing that $x = 3$ or $x = (15t^2 - 3)/(1 - 5t^2)$. Thus, the rational map

$$t \mapsto \left(\frac{15t^2 - 3}{1 - 5t^2}, t \left(\frac{15t^2 - 3}{1 - 5t^2} - 3\right)\right)$$

gives a rational parametrization of $C_1$ over $\mathbb{Q}$. In particular, $C_1(\mathbb{Q})$ is infinite. To see that $C_1(\mathbb{Z})$ is infinite, first note that if $N(x + y\sqrt{5}) = x^2 - 5y^2$ is the norm map on $\mathbb{Z}[\sqrt{5}]$, then $N(9 + 4\sqrt{5}) = 1$. For each integer $n \geq 1$, let $(x_n, y_n) \in \mathbb{Z}^2$
be such that \( x_n + y_n\sqrt{5} = 3(9 + 4\sqrt{5})^n \). The collection \( \{(x_n, y_n)\} \) is infinite since
\[
| x_n + y_n\sqrt{5} | \to \infty \text{ as } n \to \infty.
\]
Moreover, we have
\[
x_n^2 - 5y_n^2 = N(x_n - y_n\sqrt{5}) = N(3(9 + 4\sqrt{5})^n) = N(3) \cdot N(9 + 4\sqrt{5})^n = 9
\]
for all \( n \geq 1 \) by multiplicativity of the norm. This shows that \( C_1(\mathbb{Z}) \) is infinite.

(b) \( C_2(\mathbb{Z}) \) is finite. Indeed, we have \((x - 2y)(x + 2y) = 9\), showing that there are only finitely many possible choices for \((x - 2y, x + 2y)\) if \((x, y) \in \mathbb{Z}^2\), and for each such choice (say \((c_1, c_2)\)) the system of linear equations
\[
x + 2y = c_1, \quad x - 2y = c_2
\]
has at most one solution in integers \((x, y) \in \mathbb{Z}^2\).

(c) The line of slope \( t \) through \((0, 0)\) is given by the equation \( y = tx \). At its points of intersection with \( C_3 \), we have
\[
t^2x^2 = x^2(x + 1) \implies x^2(x + 1 - t^2) = 0
\]
showing that \( x = 0 \) or \( x = 1 - t^2 \). So the map
\[
t \mapsto (1 - t^2, t - t^3)
\]
gives a rational parametrization of \( C_3 \) over \( \mathbb{Q} \).

3. Exercise in \( p \)-adic disks.
(a) If \( x \in \overline{B}(2, 1) \), then \(|x - 3|_p = |(x - 2) + (-1)|_p \leq \max(|x - 2|_p, |1|_p) = 1 \), so \( x \in \overline{B}(3, 1) \). This shows \( \overline{B}(2, 1) \subseteq \overline{B}(3, 1) \), and similarly \( \overline{B}(3, 1) \subseteq \overline{B}(2, 1) \), so that \( \overline{B}(2, 1) = \overline{B}(3, 1) \) as desired. Since \(|3 - 2|_p = |1|_p = 1\), we see that \( 3 \notin B(2, 1) \) but obviously \( 3 \in B(3, 1) \), so \( B(2, 1) \neq B(3, 1) \).

(b) We have \( \overline{B}(0, 1) = \{ z \in \mathbb{Z}_p : |z|_p \leq 1 \} = \mathbb{Z}_p \). By considering \( p \)-adic expansions, for each \( x \in \mathbb{Z}_p \), there exists unique \( b \in \{1, \ldots, p - 1\} \) such that \(|x - b|_p < 1\), i.e. \( x \in B(b, 1) \). Conversely, for any \( b \in \mathbb{Z} \) we have \( B(b, 1) \subseteq \overline{B}(b, 1) = \overline{B}(0, 1) \) where the last equality follows by arguing as in part (a), noting that every integer has \( p \)-adic absolute value at most 1. This shows that in fact \( \overline{B}(0, 1) \) is a finite disjoint union of the sets \( B(0, 1), \ldots, B(p - 1, 1) \).

4. Absolute values.
(a) If \(|\cdot|\) is nonarchimedean, then for any positive integer \( n \) its image in \( K \) (also denoted \( n \)) satisfies
\[
|n| = |1 + \cdots + 1| \leq |1| = 1
\]
and similarly \(|-n| \leq 1\) since \(|-1| = 1\). This shows that \(|\cdot|\) is bounded on the image of \( \mathbb{Z} \to K \). Conversely, suppose \(|\cdot|\) is bounded above by some constant \( C \geq 0 \) on the image of \( \mathbb{Z} \) in \( K \). For any \( x, y \in K \) and any integer \( n \geq 1 \), we have
\[
|x + y|^n = |(x + y)^n| = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \leq \sum_{k=0}^{n} \binom{n}{k} |x|^{n-k} |y|^k \leq (n + 1)C \max\{|x|, |y|\}^n.
\]
This shows that
\[ |x+y| \leq (n+1)^{1/n} C^{1/n} \max\{|x|,|y|\}. \]
Letting \( n \to \infty \) and noting \( (n+1)^{1/n} C^{1/n} \to 1 \), we conclude \( |x+y| \leq \max\{|x|,|y|\} \) for every \( x,y \in K \), i.e. \( |\cdot| \) is nonarchimedean.

(b) Here, it is implicit that \( |0|_p = 0 \). Since \( k[x] \) is a Euclidean domain, the map \( |\cdot|_p \) is well-defined. Clearly, \( |f|_p = 0 \) if and only if \( f = 0 \). If \( f_1, f_2 \in k(x) \) are nonzero elements, then
\[
f_i(x) = p(x)^{-\log |f_i|_p} g_i(x) h_i(x)
\]
for some \( g_i(x), h_i(x) \in k[x] \) with \( \gcd(p(x), g_i(x)) = \gcd(p(x), h_i(x)) = 1 \) for each \( i \), by definition of \( |\cdot|_p \). We then have
\[
f_1 f_2 = p^{-(\log |f_1|_p + \log |f_2|_p)} g_1 g_2 h_1 h_2
\]
so \( |f_1 f_2|_p = e^{\log |f_1|_p + \log |f_2|_p} = |f_1|_p |f_2|_p \). If now \( |f_1|_p \geq |f_2|_p \), then
\[
f_1 + f_2 = p^{-\log |f_1|_p} g_1 h_2 - p^{-\log |f_1|_p + \log |f_1|_p} g_1 g_2 h_1 h_2
\]
and \( \gcd(p, h_1 h_2) = 1 \) since \( p \) is irreducible. Then \( |f_1 + f_2|_p \leq |f_1|_p = \max\{|f_1|_p, |f_2|_p\} \). This shows that \( |\cdot|_p \) is a nonarchimedean absolute value on \( k(x) \).

(c) Consider the map \( \deg : k(x)^\times \to \mathbb{Z} \) given by
\[
\deg \left( \frac{p(x)}{q(x)} \right) = \deg p(x) - \deg q(x)
\]
for every nonzero \( p, q \in k[x] \), where \( \deg(p) \) and \( \deg(q) \) on the right hand side are the usual degree of polynomials. We define \( \deg(0) = -\infty \). If \( p/q = r/s \) with \( p, q, r, s \in k[x] \) and \( r, s \) nonzero, then \( ps = qr \) which shows
\[
\deg(p) + \deg(s) = \deg(q) + \deg(r) \implies \deg(p/q) = \deg(r/s)
\]
by the usual property of degree on polynomials in \( k[x] \), so that \( \deg : k(x)^\times \to \mathbb{Z} \) is well-defined. (Here and in what follows, we take the convention \( a -\infty = -\infty \) for every \( a \in \mathbb{Z} \cup \{-\infty\} \).) Note that \( \deg(f) = -\infty \) if and only if \( f = 0 \). It is clear that \( \deg(fg) = \deg f + \deg g \) for every \( f, g \in k(x) \). For every \( p, q, r, s \in k[x] \) with \( q, s \) nonzero we have
\[
\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs}
\]
showing that
\[
\deg \left( \frac{p}{q} + \frac{r}{s} \right) = \deg(ps + qr) - \deg(qs)
\]
\[
\leq \max \{ \deg(p) + \deg(s), \deg(q) + \deg(r) \} - \deg(q) - \deg(s)
\]
\[
\leq \max \{ \deg(p) - \deg(q), \deg(r) - \deg(s) \} = \deg \left( \frac{p}{q} \right) + \deg \left( \frac{r}{s} \right).
\]
The above computations show that \( -\deg : k(x) \to \mathbb{Z} \cup \{+\infty\} \) is a discrete valuation. Defining the function \( |\cdot|_\infty : k(x) \to \mathbb{R}_{\geq 0} \) by \( |f|_\infty = e^{\deg |f|} \), we therefore see that \( |\cdot|_\infty \) is a nonarchimedean absolute value on \( k(x) \). Finally, we note that \( |\cdot|_\infty \) cannot be equivalent to any \( |\cdot|_p \) defined in part (b), since \( |p|_\infty > 1 \) but \( |p|_p < 1 \) for
every monic irreducible \( p \in k[x] \).

(d) Since \( \pi \) is transcendental, the map \( t \mapsto \pi \) gives an isomorphism of \( \mathbb{Q}(t) \) onto the subfield \( \mathbb{Q}(\pi) \) of \( \mathbb{R} \). The restriction of the usual absolute value to \( \mathbb{Q}(\pi) \) is clearly archimedean, and under the isomorphism above this gives an archimedean absolute value on \( \mathbb{Q}(t) \).

5. The Chevalley–Warning theorem.

(a) We claim that
\[
\sum_{x \in \mathbb{F}_q} x^n = \begin{cases} 
-1 & \text{n is a positive multiple of } q - 1 \\
0 & \text{otherwise.}
\end{cases}
\]

First, we have \( x^0 = 1 \) for every \( x \in \mathbb{F}_q \) so \( \sum_{x \in \mathbb{F}_q} x^0 = q = 0 \), verifying our claim for \( n = 0 \). Suppose next that \( 0 < n < q - 1 \). Since the equation \( x^n = 1 \) has at most \( n < q - 1 \) solutions in \( \mathbb{F}_q \) we may choose nonzero \( a \in \mathbb{F}_q \) such that \( a^n \neq 1 \). Now,
\[
a^n \sum_{x \in \mathbb{F}_q} x^n = \sum_{x \in \mathbb{F}_q} (ax)^n = \sum_{x \in \mathbb{F}_q} x^n
\]
since multiplication by \( a \) permutes the elements of the field \( \mathbb{F}_q \). This shows that
\[
(a^n - 1) \sum_{x \in \mathbb{F}_q} x^n = 0 \implies \sum_{x \in \mathbb{F}_q} x^n = 0
\]
since \( a^n - 1 \neq 0 \) in \( \mathbb{F}_q \). Finally, if \( n \geq q - 1 \), then writing \( n = m(q - 1) + r \) with integers \( m \geq 0 \) and \( 0 \leq r < q - 1 \) we have
\[
\sum_{x \in \mathbb{F}_q^*} x^n = \sum_{x \in \mathbb{F}_q^*} (x^{q-1})^m x^r = \sum_{x \in \mathbb{F}_q^*} x^r = \begin{cases} 
q - 1 & r = 0 \\
1 & r > 0
\end{cases}
\]
since \( x^{q-1} = 1 \) for every \( x \in \mathbb{F}_q^* \). This finishes the proof of our claim.

(b) Implicit below is the assumption that \( f \) has degree \( d \geq 1 \). Note that we have
\[
\sum_{P \in \mathbb{F}_q^n} (1 - f(P)^{q-1}) = \# \{ P \in \mathbb{F}_q^n : f(P) = 0 \} \text{ in } \mathbb{F}_q.
\]
We show that the left hand side is zero. Note that \( f(x_1, \ldots, x_n)^{q-1} \in \mathbb{F}_q[x_1, \ldots, x_n] \) is an \( \mathbb{F}_q \)-linear combination of monomials \( x_1^{d_1} \cdots x_n^{d_n} \) with \( d_1 + \cdots + d_n = d(q - 1) \), since \( f \) is homogeneous of degree \( d \). Since \( \sum_{P \in \mathbb{F}_q^n} 1 = q^n = 0 \), to prove that \( \sum_{P \in \mathbb{F}_q^n} (1 - f(P)^{q-1}) = 0 \) it therefore suffices to show that
\[
\sum_{(a_1, \ldots, a_n) \in \mathbb{F}_q^n} a_1^{d_1} \cdots a_n^{d_n} = \prod_{i=1}^{n} \sum_{a \in \mathbb{F}_q} a^{d_i} = 0
\]
for every choice of \( d_1, \ldots, d_n \geq 0 \) with \( d_1 + \cdots + d_n = d(q - 1) \). Since \( d < n \) by hypothesis, we have \( d_1 + \cdots + d_n < n(q - 1) \) for any choice of \( d_1, \ldots, d_n \) as above, so \( d_i < q - 1 \) for some \( i \). Then the product above must be zero by part (a). We thus conclude that \( \sum_{P \in \mathbb{F}_q^n} (1 - f(P)^{q-1}) = 0 \), and in particular the number of solutions to \( f = 0 \) in \( \mathbb{F}_q^n \) must be divisible by \( p \). This number must be nonzero since \( f(0) = 0 \), and therefore must then be \( \geq p \); this implies that \( f = 0 \) has at least one nontrivial solution, as desired.
(c) Note that the sum
\[ \sum_{P \in \mathbb{F}_q^n} \prod_{i=1}^m (1 - f_i(P)^q - 1) \]
counts the number modulo \( p \) of points \( P \in \mathbb{F}_q^n \) such that \( f_1(P) = \cdots = f_m(P) = 0 \). Expanding the product \( \prod_{i=1}^m (1 - f_i(x_1, \cdots, x_n)^q - 1) \) into a linear combination of monomials and applying the same argument as in part (b), we find that the above sum must be zero in \( \mathbb{F}_q \), and so the number of solutions to \( f_1 = \cdots = f_m = 0 \) in \( \mathbb{F}_q \) is divisible by \( p \). Since \( f_1(0) = \cdots = f_m(0) = 0 \), this number is positive and so \( f_1 = \cdots = f_m = 0 \) has a nontrivial solution in \( \mathbb{F}_q \).

(d) The polynomial \( x^2 + y^2 \) has no nontrivial zeros in \( \mathbb{F}_7 \). Indeed, the squares in \( \mathbb{F}_q \) are precisely the congruence classes \( \{0, 1, 2, 4\} \) mod 7, and if two elements in this set add up to 0 in \( \mathbb{F}_7 \) then they must be both zero.

6. Ring of profinite integers.
(a) This is routine.

(b) The inverse limit is
\[ \hat{\mathbb{Z}} = \{ (a_n) \in \prod_{n=1}^\infty (\mathbb{Z}/n\mathbb{Z}) : a_n \equiv a_m \mod n \text{ whenever } n | m \} . \]
The natural ring homomorphism \( \mathbb{Z} \to \hat{\mathbb{Z}} \) given by \( a \mapsto (a \mod n) \) must be injective, since if \( a \in \mathbb{Z} \) is an integer such that \( a \equiv 0 \mod n \) for all \( n \geq 1 \) then \( a = 0 \) (as seen by considering congruence modulo \( |a| + 1 \)).

(c) With the identification \( \mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z} \), the natural ring homomorphism
\[ \hat{\mathbb{Z}} \to \prod_{p \text{ prime}} \mathbb{Z}_p = \prod_{p \text{ prime}} \varprojlim \mathbb{Z}/p^n\mathbb{Z} \]
is given by \( (a_n) \mapsto ((a_{p^n}), (a_{p^2}), \ldots, (a_{p^e})), \ldots) \).

First, this map is injective. Indeed, suppose that the sequence \( (a_n) \in \hat{\mathbb{Z}} \) satisfies \( a_{p^e} = 0 \) in \( \mathbb{Z}_p \) for every prime \( p \), i.e. \( a_{p^e} = 0 \) in \( \mathbb{Z}/p^e\mathbb{Z} \) for \( e \geq 1 \). If \( m \geq 1 \) is an integer with prime factorization \( m = p_1^{e_1} \cdots p_r^{e_r} \), then the image \( (a_{p_1^{e_1}}, \ldots, a_{p_r^{e_r}}) \) of \( a_m \in \mathbb{Z}/m\mathbb{Z} \) under the isomorphism
\[ \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z} \]
given by the Chinese Remainder Theorem must be zero, so \( a_m = 0 \). This being true for every \( m \geq 1 \), we conclude that \( (a_n) = 0 \) in \( \hat{\mathbb{Z}} \), proving injectivity.

Second, this map is surjective. Given a sequence \( ((a_{p^n}), (a_{p^2}), \ldots, (a_{p^e})), \ldots) \) in \( \prod_{p \text{ prime}} \mathbb{Z}_p \), the Chinese remainder theorem uniquely determines an element \( a_m \in \mathbb{Z}/m\mathbb{Z} \) for each \( m \in \mathbb{Z}_{\geq 1} \), and it is clear that the sequence \( (a_n) \) forms an element in \( \hat{\mathbb{Z}} \) which maps to \( ((a_{p^n})) \).