Math 115. Number theory. May 8, 2018. Final exam

1. Let $(m,n)=1$. A yard-long log is divided by $m-1$ blue markings into m equal parts, and by $n-1$ red markings into n equal parts. Find the shortest distance between red and blue markings.

`Solution.` Clearly $|k/m-l/n|\geq 1/mn$, unless $k/m=l/n$, which doesn't happen inside the log since $(m,n)=1$. For some $k,l\in\mathbf{Z}$ we have $kn-lm=1$, and hence $k/m-l/n=1/mn$, i.e. the distance $1/mn$ can be achieved between blue and red markings k/m and l/n made on an infinite log at *non-integer* points. Obviously integer points cannot fit such a short interval, since the closest distance from k/m (resp. l/n) to an integer is $1/m$ (resp. $1/n$), which is greater than $1/mn$. Thus, cutting the infinite log at integer points into logs of length 1, we conclude that some (and hence all) of the copies contain the markings at the distance $1/mn$.

2. Show that 2 is a primitive root $\mod 3^{2018}$ (i.e. powers of 2 represents all congruence classes coprime to 3^{2018}).

`Solution.` By Euler's theorem, $2^{\phi(3^{2018})}\equiv 1 \mod 3^{2018}$, and we need to show that $2^d\not\equiv 1 \mod 3^{2018}$ for any proper divisor d of $\phi(3^{2018})=2\cdot 3^{2017}$. When $d=3^k$, then $2^d\equiv -1 \mod 3$ since 3^k is odd, and $2\equiv -1 \mod 3$. When $d=2\cdot 3^k$, we show by induction on k that $2^d\equiv 1+3^{k+1} \mod 3^{k+2}$. Indeed, for $k=0$ we have $2^2=1+3$. For $k>0$, from the binomial formula $(1+x)^3=1+3x+3x^2+x^3$, we derive $(1+3^k+o(3^k))^3=1+3^{k+1}+o(3^{k+1})$ where $o(3^l)$ denotes terms divisible by 3^{l+1}. Thus $2^d\not\equiv 1 \mod 3^{2018}$ as long as k remains smaller than 2017.

3. For a prime p such that $p\equiv -1 \mod 3$, prove that every congruence class $\mod p$ has a unique cube root.

`Solution.` Since $p-1$ is not divisible by 3, the cube function $\mathbf{Z}_p\to\mathbf{Z}_p : x\mapsto x^3$ is bijective. In abstract algebra terms this is obvious since $\mathbf{Z}_p$ cannot have elements of order 3. But even without abstract algebra, it is made obvious by representing $x\not\equiv 0 \mod p$ as a^k where a is a primitive root. For, in terms of the exponents k the fact reduces to the statement that $\mathbf{Z}_{p-1}\to\mathbf{Z}_{p-1} : k\mapsto 3k$ is bijective (i.e. that $(3,p-1)=1$, which is true).

4. For the Möbvious function μ, prove that $\sum_{d|n}\mu(d)=0$ for all $n>1$, and derive (assuming $s>1$) that $1/\zeta(s)=\sum_{n\geq 1}\mu(n)/n^s$.

`Solution.` For a direct proof (not using the multiplicative property of μ), we note that for $n=p_1^{k_1}\cdots p_r^{k_r}$, $\mu(p_{i_1}\dots p_{i_l})=(-1)^l$ (here p_{i_j} are distinct

primes), and $\mu(d) = 0$ for all other $d|n$. Thus $\sum_{d|n} \mu(d) = \sum_{l=0}^{r} \binom{r}{l}(-1)^l = (1-1)^r$ by the binomial formula. This is 0 if $r > 0$ (i.e. $n > 1$), and 1 when $r = 0$ (i.e. $n = 1$). Now, $\zeta(s) := \sum_{m\geq 1} 1/m^s$ for $s > 1$, and so $\zeta(s)\left[\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right] = \sum_{m,n\geq 1} \frac{\mu(n)}{(mn)^s} = \sum_{N\geq 1} \frac{\sum_{n|N} \mu(n)}{N^s} = 1$.

5. $a^{13} \equiv 2 \mod 59$. Find $a \mod 59$.

`Solution.` Since 59 is prime, $a^{58} \equiv 1 \mod 59$ by Fermat's little theorem. We have: $58 = 4 \cdot 13 + 6$, $13 = 2 \cdot 6 + 1$, and hence $1 = 13 - 2 \cdot 6 = 13 - 2(58 - 4 \cdot 13) = 9 \cdot 13 - 2 \cdot 58$. Thus, $9 \cdot 13 \equiv 1 \mod 58$, and hence $2^9 = a^{13 \cdot 9} \equiv a \mod 59$. We have: $2^9 = 512 = 8 \cdot 59 + 40$, i.e. $a \equiv 40 \equiv -19 \mod 59$.

6. Show that the *Gauss–Givental* ring $\mathbf{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbf{Z}\}$ is not Euclidean (with respect to the norm $N(a + b\sqrt{-3}) = a^2 + 3b^2$ in $\mathbf{Q}(\sqrt{-3})$), and find an example of non-unique factorization in this ring.

`Solution.` In the rectangle with the vertices $0, 1, \sqrt{3}i, 1 + \sqrt{3}i$ on the complex plane, the center $(1 + \sqrt{3}i)/2$ is distance 1 away from all the four vertices (and ever farther from all other elements of the lattice). This shows that the Euclidean property does not hold. For instance (multiply by 2): $1 + \sqrt{3}i$ is distance ≥ 2 away from all multiples of 2 in $\mathbf{Z}[\sqrt{-3}]$. Since $2 \neq a^2 + 3b^2$, the equality $(1 + \sqrt{3}i)(1 - \sqrt{3}i) = 2 \cdot 2$ provides two different factorizations of 4 into irreducible (but non-prime) factors. The irreducibility follows from $N(2) = N(1 \pm \sqrt{-3}) = 4$ being not factorable into smaller values of the norm. In fact such non-uniqueness alone (without the previous geometric argument) already implies that the ring is not Euclidean.

7. Find out which of the primes between 20 and 50 can occur among divisors of the sequence of integers $a_n := n^2 + n - 3$, $n = 0, \pm 1, \pm 2, \ldots$

`Solution.` Solving $a_n \equiv 0 \mod p$ by a quadratic formula, we find $n \equiv (-1 \pm \sqrt{13})/2 \mod p$, which yields a solution whenever $\left(\frac{13}{p}\right) = 1$. By the quadratic reciprocity, this is equivalent to p being one of the quadratic residues $\pm 1, \pm 4, \pm 3 \mod 13$. The primes $p = 23, 29, 31, 37, 41, 43, 47$ between 20 and 50 are congruent respectively to $-3, 3, 5, -2, 2, 4, -5 \mod 13$. Therefore from this range only $p = 23, 29, 43$ occur among the divisors of a_n.

8. Find out whether the sets of integers representable by the binary quadratic forms $4x^2+9xy+7y^2$ and $5x^2+17xy+16y^2$ (both with discriminant -31) coincide.

`Solution.` Using the algorithm of reducing the forms, we have:

$$4(x-y)^2+9(x-y)y+7y^2 = 4x^2+xy+2y^2 \mapsto 2x^2-xy+4y^2 \text{ (reduced)}$$
$$5(x-y)^2+17(x-y)y+16y^2 = 5x^2+7xy+4y^2 \mapsto 4x^2-7xy+5y^2 \mapsto$$
$$4(x+y)^2-7(x+y)y+5y^2 = 4x^2+xy+2y^2 \mapsto 2x^2-xy+4y^2 \text{ (reduced)}$$

Thus the forms are equivalent, and hence the sets of their values coincide.

9. Compute the quadratic irrational given by the purely periodic continued fraction $[\overline{1,1000}] = [1,1000,1,1000,\dots]$ with the precision of 10^{-9}.

`Solution.` The convergent $p_1/q_1 = [1,1000,1] = 1002/1001$ has the denominator $q_1 = 1001$. The denominator of the next convergent will have the form $q_2 = 1000q_1+q_0 > 10^6$. Therefore the error of the approximation by p_1/q_1 is $< 1/q_1q_2 < 10^{-9}$. In the decimal form, $1002/1001 = 1.\overline{000999}$, and hence the rounding 1.000999001 will provide the required approximation.

10. Find the smallest solution of Pell's equation $x^2-19y^2=1$ in positive integers (x,y), and use it to describe all units in the ring of algebraic integers of the quadratic field $\mathbf{Q}(\sqrt{19})$.

`Solution.` We are looking for the continued fraction expansion of $\sqrt{19}$ until the beginning of the period: $\sqrt{19} = 4+(\sqrt{19}-4)$,

$$\frac{1}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{3} = 2+\frac{\sqrt{19}-2}{3}$$
$$\frac{3}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{5} = 1+\frac{\sqrt{19}-3}{5}$$
$$\frac{5}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{2} = 3+\frac{\sqrt{19}-3}{2}$$
$$\frac{2}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{5} = 1+\frac{\sqrt{19}-2}{5}$$
$$\frac{5}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{3} = 2+\frac{\sqrt{19}-4}{3}$$
$$\frac{3}{\sqrt{19}-4} = \sqrt{19}+4 = 8+(\sqrt{19}-4)$$

Thus $\sqrt{19} = [4,\overline{2,1,3,1,2,8}]$ with the period of even length 6. The general theory now says that Pell's equation $x^2-19y^2=-1$ has no solutions, and

the minimal positive solution (x, y) to $x^2 - 19y^2 = +1$ is represented by the convergent $x/y = [4, 2, 1, 3, 1, 2]$. We compute: 2; $1 + 1/2 = 3/2$; $3 + 2/3 = 11/3$; $1 + 3/11 = 14/11$; $2 + 11/14 = 39/14$; $4 + 14/39 = 170/39$. Thus, $(x, y) = (170, 39)$. Now the general theory says that all solutions come from the sequence $x + y\sqrt{19} = \pm(170 + 39\sqrt{19})^k$, $k = 0, \pm 1, \pm 2, \ldots$. Since $19 \equiv 3 \mod 4$, algebraic integers in $\mathbf{Q}(\sqrt{19})$ have the form $x + y\sqrt{19}$ with $x, y \in \mathbf{Z}$, and the units exactly correspond to the elements of norm $x^2 - 19y^2 = \pm 1$, i.e. the unita *are* the terms of the above sequence.