MATH 4123 HISTORY OF MATHEMATICS
PROF. PAUL BAILEY

Problem Set 2
November 5, 2008

Solutions

Problem 1. Using straightedge and compass, construct an angle of 54°. Describe each step, discussing why your construction is effective.

Solution. Construct a 72° angle as per previous instructions. The supplementary angle is 108°. Bisect this to obtain 54°. □

Definition 1. Let $m, n \in \mathbb{Z}$. The *least common multiple* of m and n is a positive integer $l \in \mathbb{Z}$ such that

(a) $m \mid l$ and $n \mid l$;

(b) $m \mid k$ and $n \mid k$ implies $l \mid k$.

Definition 2. Let $n \in \mathbb{Z}$ with $n \geq 2$. Set $\mathbb{Z}_n = \{r \in \mathbb{Z} \mid 0 \leq r < n\}$. Define a function

$$\rho_n : \mathbb{Z} \to \mathbb{Z}_n \quad \text{by} \quad \rho_n(a) = \text{ the remainder when } a \text{ is divided by } n.$$

We call ρ the *residue map*.

Definition 3. Let $m, n \in \mathbb{Z}$ with $m \geq 2$, $n \geq 2$. Define a function

$$\sigma_{m,n} : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \quad \text{by} \quad \sigma_{m,n}(a) = (\rho_m(a), \rho_n(a)).$$

We call σ the *joint residue map*.

Problem 4. Let $m, n \in \mathbb{Z}$ with $m \geq 2$ and $n \geq 2$. Let $d = \gcd(m, n)$ and $l = \operatorname{lcm}(m, n)$.

(a) Show that if $d = 1$, then $\sigma_{m,n}$ is bijective.

(b) Show that if $a \equiv b \pmod{l}$, then $\sigma_{m,n}(a) = \sigma_{m,n}(b)$.

Proof. Fix m and n and let $\sigma = \sigma_{m,n}$. We note that $|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$. By a previous theorem, $\rho_n(a) = \rho_n(b)$ if and only if $a \equiv b \pmod{n}$.

(a) Let $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Since $\gcd(m, n) = 1$, the Chinese Remainder Theorem tells us that there exists $c \in \mathbb{Z}$ such that $a \equiv c \pmod{m}$ and $b \equiv c \pmod{n}$, that is, $\rho_m(c) = a$ and $\rho_n(c) = b$. Moreover, this c may be selected so that $0 \leq c < mn$; select c from $\mathbb{Z}_{mn}$. Then $\sigma(c) = (a, b)$, and σ is surjective. A surjective function between finite sets of the same cardinality is necessarily injective, so σ is bijective.

(b) Suppose k is a common multiple of m and n. Then there exist $x, y \in \mathbb{Z}$ such that $mx = k$ and $ny = k$.

We assume that $a \equiv bg \pmod{k}$, so $k \mid a - b$, and $a - b = kz$ for some $z \in \mathbb{Z}$. Thus $a - b = mxz$ and $a - b = nyz$. Thus $m \mid a - b$ and $n \mid a - b$. Therefore $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. □

Problem 2. Compute the volume of a regular icosahedron inscribed in a sphere of radius 1.

Solution. We proceed as follows.

(a) Find an icosahedron inscribed in a sphere.

(b) Find the area A of one face.

(c) Find the length h of the apothem (the distance from the center of the sphere to the centroid of a face).

(d) The volume of the tetrahedron whose base is a face and whose apex is the center of the sphere is $\frac{1}{3}Ah$. There are 20 faces, so the volume I of the entire icosahedron is $\frac{20Ah}{3}$.

(e) Find the radius r of the sphere.

(f) Find the volume V of the icosahedron inscribed in a unit sphere, which is $\frac{20Ah}{3r^3}$.

(a) *Find an icosahedron.* Let $\phi = \frac{1+\sqrt{5}}{2}$. Then $\phi^2 = \phi - 1$.
The twelve points $(\pm\phi, \pm 1, 0)$, $(\pm 1, 0, \pm\phi)$, $(0, \pm\phi, \pm 1)$, form the vertices of a regular icosahedron in $\mathbb{R}^3$.
(b) *Find the area A of one face.* Consider the face with vertices $(\phi, \pm 1, 0)$ and $(1, 0, \phi)$. The area of an equilateral triangle with edge length e is

$$A = \frac{1}{2}e(e\sin 60^\circ) = \frac{e^2\sqrt{3}}{4}.$$

The length of one side is distance between the first to vertices, which is

$$e = \sqrt{(\phi - \phi)^2 + (1 - (-1))^2} = \sqrt{4} = 2.$$

Thus $A = \sqrt{3}$.
(c) *Find the length h of the apothem.* The center of the sphere is the origin. The centroid is the average of the coordinates of the vertices, which is $(\frac{2\phi+1}{3}, 0, \frac{\phi}{3})$. The apothem is

$$h = \frac{1}{3}\sqrt{(2\phi+1)^2 + \phi^2}.$$

We note that

$$2\phi + 1 = \phi^2 + \phi = \phi(\phi + 1) = \phi^3.$$

Thus

$$(2\phi+1)^2 + \phi^2 = 5\phi^2 + 4\phi + 1 = 3\phi(2\phi+1) = 3\phi^4.$$

Therefore

$$h = \frac{1}{3}\sqrt{3\phi^4} = \frac{\phi^2}{\sqrt{3}}.$$

(d) *Find the volume of the tetrahedron.* We have

$$I = \frac{20Ah}{3} = \frac{20(\sqrt{3})(\phi^2/\sqrt{3})}{3} = \frac{20\phi^2}{3}.$$

(e) *Find the radius of the sphere.* This is the distance from the origin to a vertex, say $(1, 0, \phi)$. We have

$$r = \sqrt{\phi^2 + 1}.$$

Thus

$$V = \frac{20\phi^2}{3\sqrt{(\phi^2+1)^3}}.$$

□

Problem 3. Consider the elliptic curve given by the equation

$$y^2 = x^3 - 12x + 25.$$

Find as many rational points on this curve as you can, including all rational points that lie on a horizontal tangent. Justify your answer.

Solution. An *elliptic curve* is the locus to an equation of the form $y^2 = f(x)$, where $f(x)$ is a cubic polynomial. Elliptic curves play a critical role in advanced arithmetic geometry.

Let $f(x) = x^3 - ax + b$; we investigate methods to find critical points on the curve $C : y^2 = f(x)$.

If we find one rational point on C, then we can use it to reduce our (difficult) cubic equation to a (tractable) quadratic equation; however, we have no guarantee that this quadratic will yield rational results. On the other hand, if we have a double rational zero or two rational zeros of a cubic equation, we can reduce the quadratic to a linear equation, whose solution will necessarily be rational. Is is the tactic employed by Diophantus.

Let (p, q) be a rational point on C. Implicit differentiation gives the slope of the tangent line at this point to be

$$m = \frac{3p^2 - a}{2q}.$$

The line through this point is

$$L : y = mx + (q - mp).$$

We intersect the line L with the curve C.

Thus, for points on this line, we have $y^2 = m^2x^2 + 2m(q - mp)x + (q - mp)^2$. If $g(x) = m^2x^2 + 2m(q - mp) + (q - mp)^2$, then $f'(p) - g'(p) = 0$, so $f - g$ has a horizontal tangent at $x = p$; therefore, p is a double zero of $f - g$. In other words, L intersects C is at most one point other than (p, q).

Let $h(x) = f(x) - g(x) = x^3 - m^2x^2 + (2m^2p - 2mq - a) + (b - (q - mp)^2)$. We divide $h(x)$ by $(x - p)^2$ (using synthetic division, we divide by p twice) and find that the quotient is $x + 2p - m^2$. Therefore, $x = m^2 - 2p$ is another zero of $h(x)$; it is the x-coordinate of the other intersection point of L and C. The y-coordinate is obtained by plugging x into the line L, and we get $y = m(m^2 - 2p) + (q - mp)$. Thus, we have found another rational point:

$$\text{By the tangent method: } m = \frac{3p^2 - a}{2q} \text{ giving } (m^2 - 2p, m^3 - 3mp + q).$$

Let (p_1, q_1) and (p_2, q_2) be rational points on C. Let

$$m = \frac{q_2 - q_1}{p_2 - p_1}.$$

Let $L : y = mx + (q_1 - mp_1)$. Again intersect L with C to construct h as above, and factor out $(x - p_1)$ and $(x - p_2)$. You will find that $x = m^2 - p_1 - p_2$ is the x-coordinate of the third point of intersection, and the corresponding y-coordinate is $m(x - p_1) + q_1$.

$$\text{By the secant method: } m = \frac{q_2 - q_1}{p_2 - p_1} \text{ giving } (m^2 - p_1 - p_2, m^3 - 2mp_1 - p_2 + q_1).$$

Of course, it is fruitless to attempt to use the secant method on a pair of points where one has been derived from the other from the tangent method.

Now having developed these formulae, it was relatively easy to write a computer program to guess easy integer solutions and search for additional rational points using the tangent and secant method. The program first searches for solutions for x between -9 and 9, then builds up a list of all points found from these whose numerator and denominator have absolute value less than 10 million. □

Here is the source listing for the program to find rational points on $y^2 = x^3 - ax + b$.

```
// Find rational points on elliptic curve y^2 = x^3 - ax + b

#include <stdio.h>
#include <math.h>
#include "Rational.h"

// Find rational points on elliptic curve y^2 = x^3 - ax + b

Rational points[100][2];
int pointc=1;

Integer abs(Integer p)
{ if (p<0) return -p;
  return p; }

int find(Rational p)
{ int k=1;
  while (k<pointc)
  { if (points[k][0] == p) return k;
    k++; }
  return 0; }

int check(Rational p)
{ if (abs(p.Getm())>10000000 || abs(p.Getn())>10000000) return 1;
  return 0; }

int put(Rational p,Rational q)
{ if (pointc>98) return 1;
  if (find(p)) return 2;
  if (check(p)) return 3;
  if (check(q)) return 4;
  points[pointc][0] = p;
  points[pointc][1] = q;
  pointc++;
  printf("(%s,%s)\n",p.String(),q.String());
  return 0; }

int tangent(Rational a,Rational b,Rational p,Rational q)
{ Rational m,x,y;
  m = (3*p*p - a)/(2*q);
  x = m*m - 2*p;
  y = m*(x-p)+q;
  if (put(x,y)) return 0;
  return 1; }

int secant(Rational a,Rational b,Rational p1,Rational q1,Rational p2,Rational q2)
{ Rational m,x,y;
  m = (q2-q1)/(p2-p1);
  x = m*m - p1 - p2;
  y = m*(x-p1)+q1;
  if (put(x,y)) return 0;
  return 1; }
```

```
int search(Rational a,Rational b)
{ int i=0,j=0,k=0;
  Rational p1,q1,p2,q2,p,q;
  for (i=1; i<pointc-1; i++)
  { for (j=i+1; j<pointc; j++)
    { p1 = points[i][0];
      q1 = points[i][1];
      p2 = points[j][0];
      q2 = points[j][1];
      k += secant(a,b,p1,q1,p2,q2); } }
  for (i=1; i<pointc; i++)
  { p = points[i][0];
    q = points[i][1];
    k+= tangent(a,b,p,q); }
  return k; }

void elliptic(Integer a,Integer b)
{ Integer x,y,z;
  for (x=-9; x<=9; x++)
  { z = x*x*x - a*x + b;
    y = squr(z);
    if (y*y != z) continue;
    put(x,y); }
  while (search(a,b)); }

int main(int argc, char* argv[])
{ elliptic(12,25);
return 0; }
```

The output of the program is a list of the rational points it found.

```
(-4,3)
(-1,6)
(0,5)
(2,3)
(3,4)
(6,13)
(8,21)
(17/4,57/8)
(50/49,1275/343)
(-7/4,51/8)
(-38/9,17/27)
(-157/49,1896/343)
(152/121,4593/1331)
(-26/9,161/27)
(14/25,537/125)
(116/49,1077/343)
(1911/361,71878/6859)
(1529/5776,2051571/438976)
(-159/64,3217/512)
(36/25,409/125)
(-3592/1681,-440691/68921)
(-13192/3721,1088151/226981)
(-3382/961,-144861/29791)
(-663/2116,-521717/97336)
(16409/4624,1636989/314432)
(8018/1681,601941/68921)
(208/9,2969/27)
(2922/169,155137/2197)
(7728/2809,532831/148877)
(41/16,213/64)
(3014/3721,902559/226981)
(275,-4560)
(-1954/3025,948219/166375)
(122,1347)
(276/169,6863/2197)
(10225/324,-1028105/5832)
(44,291)
(14,51)
(1271/361,35238/6859)
(1124/289,29949/4913)
(7952/841,-670983/24389)
```