Number Theory Exam B

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
3 August, 2016 (at *21:17*)

B0: Make up, or find, your own interesting, elegant, NT problem, then solve it. Aesthetics counts. Make sure that the problem has some genuine mathematical interest, and genuine mathematical difficulty. Important: Make sure that it really uses some Number *Theory*, not just uses numbers! [*E.g,* a problem which significantly uses some of our theorems or algorithms is one possible criterion.]

B1: Recall that ***sympoly*** means "symmetric polynomial". A Write-out the lowest degree, simplest, sympoly $Y(a,b,c)$, so that $Y(a,b,c)$ is zero IFF one of the numbers a,b,c is equal to the sum of the other two.

B Explicitly write Y in the form

1: $$Y = \mathsf{q}_1 S_{\alpha_1} + \mathsf{q}_2 S_{\alpha_2} + \cdots + \mathsf{q}_K S_{\alpha_K},$$

where each α_k is an N-profile. (What is the value of N, and why?) Furthermore $\alpha_1 \succ \alpha_2 \succ \ldots \succ \alpha_K$, lexicographically, and each $\mathsf{q}_k \in \mathbb{Z}$ with $\mathsf{q}_k \neq 0$.

C Compute, showing all the steps, the unique polynomial $F(s_1,\ldots,s_N)$ such that

$$F\big(\sigma_1(a,b,c),\ldots,\sigma_N(a,b,c)\big) = Y(a,b,c).$$

Recall that $\sigma_1,\ldots,\sigma_N$ are the *elementary symmetric polynomials.* [*Advice:* Check your answer.]

D Now consider a cubic poly

$$g(x) = x^3 + Ex^2 + Dx + C.$$

Let a,b,c denote the three roots of g. Viewing $F(\sigma_1,\ldots,\sigma_N)$ as a function of these three roots, write an explicit poly

$$\mathrm{W}(E,D,C)$$

which equals $F(\sigma_1,\sigma_2,\sigma_3)$. Call the resulting number the ***weird discriminant*** of g.

Compute the weird discriminant of each of the following polys, saying which polys are ***weird***; that is, have one root equal to the sum of the two other roots.

$$g_1(x) := x^3 - 12x^2 + 45x - 54;$$
$$g_2(x) := x^3 - 2[1+\sqrt{2}]x^2 + 3[1+\sqrt{2}]x - [2+\sqrt{2}];$$
$$g_3(x) := x^3 + 17.$$

B2: Let $\mathbf{E}$ denote the (*familiar!*) elliptic curve

2: $$x^3 + 17 = y^2 \quad (\text{with } x,y \in \mathbb{R})$$

together with its point at ∞. Then $P := (-2,-3)$ and $Q := (-1,4)$ are points on $\mathbf{E}$.

i As described in class, compute the point $(c,d) := P \cap Q$, where $c,d \in \mathbb{R}$. I.e, write the line $\overline{PQ}$ as

3: $$y = M[x - A] + B,$$

with A,B,M real. Plug this into (2) and rewrite as

2′: $$f(x) = 0,$$

where f is a monic cubic polynomial. Argue that the quotient

$$\frac{f(x)}{[x - {-2}][x - {-1}]}$$

is a *polynomial*, is monic, and has degree 1. Now compute c, then d.

Letting $\oplus$ denote the group-addition on $\mathbf{E}$, recall that $P \oplus Q$ is the point $(c,-d)$. Your value of $P \oplus Q$ will involve three digit integer(s), but no larger. [*Hint:* To check your method, here is the result when I change P to $P' := (-2,3)$. Then $P' \oplus Q$ equals $(4,-9)$.]

ii Now please show all the steps to compute the point $Q \oplus Q$. One approach is as above except that, instead of the line $\overline{PQ}$, you will use the tangent-line to $\mathbf{E}$ at Q (which is what $\overline{PQ}$ becomes if we slide P along $\mathbf{E}$ to Q). [*Hint:* The tangent-line can be found by implicit differentiation.] Another approach is to compute $\lim_{P \to Q}[P \oplus Q]$.

B3: Define two polynomials

$$f(a,b,c) \;:=\; a^2c + 4ab + 3c + 1\,;$$
$$h(w,x,y) \;:=\; x + 4wy + 3xy^2 + y^3\,.$$

Define two triples

$$\vec{u} := \big(a,b,c\big) := \big(\text{-}4,6,5\big)\,;$$
$$\vec{v} := \big(w,x,y\big) := \Big(\frac{-3}{2},\frac{-5}{4},\frac{-1}{4}\Big)\,.$$

Verify that $\vec{u}$ is a zero of f and that $h(\vec{v}) = 0$. In some sense, these two solutions "correspond".

How? Say that $\vec{u}$ is a ***good*** ***f-triple*** if $f(\vec{u}) = 0$, each of a,b,c is rational and a is non-zero. Further, $\vec{v}$ is a ***good*** ***h-triple*** if $h(\vec{v}) = 0$, each of w,x,y is rational and [*Splatch!* `Variable unreadable`] is non-zero.

Please derive a formula for a function

$$\Phi\colon\{\text{Good } f\text{-triples}\}\to\{\text{Good } h\text{-triples}\}$$

which is a bijection. (The formula will have, f'irinstance, x as a rational fnc of a,b,c.) Naturally, your formula should have that $\Phi(\vec{u}) = \vec{v}$.

Give a formula for Λ, the inverse function of Φ. Make sure to say explicitly what was the *Splatched!* variable up above. [*Hint:* As we did in the extra class, homogenize f to

$$g(a,b,c,z) \;:=\; z^3\cdot f\big(\tfrac{a}{z},\tfrac{b}{z},\tfrac{c}{z}\big)\,.$$

Now dehomogenize in some different way, then rename the variables.]

Do you see that two *different* polys might have the same "rational Number Theory", because they are different realizations of the same homogeneous polynomial in Projective Coordinates? Can you take this idea somewhere?

End of N.T. Exam B

Bonus: In the elliptic curve problem, show by explicit computation that

$$P\oplus[Q\oplus Q] \;=\; [P\oplus Q]\oplus Q\,.$$

Thus you will have shown, in this one case, that $\oplus$ is associative.

Folks, this was a terrific class for me, and I appreciate your contribution. Please stop by next semester to tell me what you are doing.

Sincerely, Jonathan King

Filename: `Classwork/NumberThy/NT2001g/b-hm.NT2001g.latex`
As of: *Wednesday 03Aug2016.* Typeset: *3Aug2016 at 21:17.*