Number Theory Exam B

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@math.ufl.edu
Webpage http://www.math.ufl.edu/~squash/

15 April, 2001

Hello. This exam is due **4PM, Tuesday, 02May2001**. To hand in your WU (write-up), **slide it under my office door**, Little Hall 402, and then *send me email* that you have done so. If you will be handing it in late, then *send me email telling me that*. (Losing a few points, I will accept your WU through noon of Wednesday, 03May.)

Whether you type your WU or write it neatly, only use *every third line*. Write in complete English sentences, and use (captioned) diagrams where appropriate.

Final instruction: *Do a good, thorough, job!*

B0: [45pts] 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: [55pts] 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

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

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

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

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.

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

B2: [35pts] Let $\mathbf{E}$ denote the (*familiar!*) elliptic curve

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

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

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

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

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

$$2': \qquad f(x) \;=\; 0\,,$$

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 $P' \coloneqq (-2,3)$. Then $P' \oplus Q$ equals $(4,-9)$.]

B3: [20pts] Define two polynomials

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

Define two triples

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

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

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

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

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

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 the steps to compute the point $Q \oplus Q$. The method 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.]

HONOR CODE: *"I have neither requested nor received help on this exam other than from my professor (or his assistant)."*

Signature:

B0:	___ ___	45pts
B1:	___ ___	55pts
B2:	___ ___	35pts
B3:	___ ___	20pts
Bonus:	___ ___	10pts
Total:	___ ___ ___	155pts

Please PRINT your Name:

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.latex`
As of: *Wednesday 25Apr2001.* Typeset: *15Apr2001* at *17:21.*