MAT 311 Number Theory
Stony Brook University
Problem Set 9 Due Thurs. 04/28/2011

Jason Starr
Spring 2011

MAT 311 Problem Set 9

Problems. Read through all of the following problems. Do at least **four** of the following six problems. If you choose to write up the solutions to more than four, please indicate which ones you want graded for credit. Also if one of your four problems makes reference to a problem you choose not to do, you *are* allowed to use the result of that problem to solve your problem.

(1) We have seen that for positive integers a, b, c with $a = bc$, if both a and b are sums of two squares, then also c is a sum of two squares (allowing 0 as one of the squares). Give an example of positive integers a, b, and c (each less than 50 for simplicity) such that $a = bc$, such that a and b are each sums of three squares, but such that c is not a sum of three squares (again allowing 0 among the squares).

(2) A polynomial $f(x_1, \ldots, x_n)$ is *homogeneous of degree* d if for every scalar c, $f(cx_1, \ldots, cx_n)$ equals $c^d f(x_1, \ldots, x_n)$. For a prime number p, a homogeneous polynomial $f(x_1, \ldots, x_n)$ with integer coefficients is said to have a *nontrivial local solution at* p if for every integer $m \geq 0$, there exist integers $(u_1, \ldots, u_n)$ (depending on f, p and m) such that both

(i) $(u_1, \ldots, u_n) \not\equiv 0 \pmod{p}$, i.e., at least one of the integers u_i is relatively prime to p, and

(ii) $f(u_1, \ldots, u_n) \equiv 0 \pmod{p^m}$.

(2.a) Assume that for every integer $m \geq 0$ there exists an integer $e \geq 0$ and integers $(u_1, \ldots, u_n)$ such that both

(i) $(u_1, \ldots, u_n) \not\equiv 0 \pmod{p^{e+1}}$, i.e., at least one of the integers u_i is not divisible by p^{e+1}, and

(ii) $f(u_1, \ldots, u_n) \equiv 0 \pmod{p^{m+de}}$.

Then prove that $f(x_1, \ldots, x_n)$ has a nontrivial local solution at p.
Hint. What power of p divides the greatest common divisor c of $(u_1, \ldots, u_n)$. What happens with f when you factor this out?

(2.b) Let S and T be $n \times n$ matrices with integer entries such that $T \cdot S = S \cdot T = c\mathbf{Id}_{n\times n}$ where $c = p^e b$ with b relatively prime to p. For every ordered n-tuple of integers $(v_1, \ldots, v_n)$, consider the linear change of coordinates $(u_1, \ldots, u_n)^\dagger = T(v_1, \ldots, v_n)^\dagger$. And define the degree d, homogeneous, integer coefficient polynomial $g(v_1, \ldots, v_n)$ by $g(v_1, \ldots, v_n) = f(u_1, \ldots, u_n) = f(T \cdot (v_1, \ldots, v_n))$. Assuming f has a nontrivial local solution at p, prove that also g has a nontrivial local solution

at p. Since also $(p^e b)^d f(u_1, \dots, u_n) = c^d f(u_1, \dots, u_n) = g(S(u_1, \dots, u_n))$, it follows that f has a nontrivial local solution at p if and only if g has a nontrivial local solution at p.
Hint. If $(w_1, \dots, w_n)$ is an ordered n-tuple of integers such that $(w_1, \dots, w_n) \not\equiv (0, \dots, 0) \pmod{p}$, what can you conclude about $(v_1, \dots, v_n) = S(w_1, \dots, w_n)$ modulo p^{e+1}? Also if $f(w_1, \dots, w_n) \equiv 0 \pmod{p^m}$, what can you conclude about $g(v_1, \dots, v_n)$ modulo p^{m+de}? Now what does **Problem (2.a)** say?

(2.c) A degree d, homogeneous, integer coefficient polynomial f is said to satisfy the *Hasse principle* if whenever there exists a nontrivial real solution as well as a nontrivial local solution at p for every prime p, then also there exists a nontrivial integer solution. Logically, this is equivalent to saying that either f has a nontrivial integer solution, or it fails to have a nontrivial real solution, or it fails to have a nontrivial local solution at p for some prime p. With notation as above, prove that f has a nontrivial integer solution, respectively nontrivial real solution, if and only if g has a nontrivial integer solution, resp. nontrivial real solution. Combined with **Problem (2.b)**, conclude that f satisfies the Hasse principle if and only if g satisfies the Hasse principle.

(3) Let $f(x_1, x_2, x_3)$ be a integer, ternary quadratic form which is in "Legendre diagonal form", i.e.,

$$f(x_1, x_2, x_3) = a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2,$$

for nonzero integers a_1, a_2, a_3 such that $a_1 a_2 a_3$ is a square-free integer.

(3.a) Prove that $f(x_1, x_2, x_3)$ has a nontrivial real solution if and only if at least one of $-a_1 a_2$, $-a_1 a_3$, $-a_2 a_3$ is positive.

(3.b) Let p be a prime divisor of a_3. Let (u_1, u_2, u_3) be a triple of integers such that both

(i) $(u_1, u_2, u_3) \not\equiv (0, 0, 0) \pmod{p}$, and

(ii) $f(u_1, u_2, u_3) \equiv 0 \pmod{p^2}$.

Prove that $(u_1, u_2) \not\equiv (0, 0) \pmod{p}$. Conclude that $-a_1 a_2$ is a square modulo p. Finally, using the Chinese Remainder Theorem, conclude that $-a_1 a_2$ is a square modulo $|a_3|$ provided that for every prime divisor p of a_3, f has a nontrivial local solution at p.

(3.c) Combine **(3.a)** and **(3.b)** to conclude that f satisfies the Hasse principle. Finally, for an arbitrary integer, ternary quadratic form g, combine this with the Gram-Schmidt algorithm and **Problem 2** to conclude that g satisfies the Hasse principle: either the Gram-Schmidt algorithm produces a nontrivial integer solution of g (so that g satisfies the Hasse principle) or else it produces change of basis matrices S and T such that $g(v_1, v_2, v_3) = qf(T(u_1, u_2, u_3))$ for a nonzero rational number q and an integer, ternary quadratic form f in Legendre diagonal form.

(4) Let $f(x_1, \dots, x_n)$ be a degree d, homogeneous, integer coefficient polynomial which has nontrivial real solutions and which has nontrivial local solutions at p for every prime p. (Technically we should also assume that the only critical point of $f(x_1, \dots, x_n)$ is the trivial zero $(0, \dots, 0)$, but this is immaterial for what follows). The polynomial f is said to satisfy *weak approximation* (at finite primes p) if for every finite collection of distinct primes $(p_1, \dots, p_r)$ and for every integer m, there exists an integer M (depending on $(p_1, \dots, p_r)$ and m) such that for every collection $((u_{1,1}, \dots, u_{1,n}), \dots, (u_{r,1}, \dots, u_{r,n}))$ of integers satisfying both

(i) $(u_{i,1}, \dots, u_{i,n}) \not\equiv (0, \dots, 0) \pmod{p_i}$, and

(ii) $f(u_{i,1}, \dots, u_{i,n}) \equiv 0 \pmod{p_i^M}$

for every $i = 1, \dots, r$, there exists an ordered n-tuple of integers $(u_1, \dots, u_n)$ (depending on m, on $(p_1, \dots, p_r)$, and on the collection $(u_{i,j})$ of M^{th}-order approximate local solutions at p_i) satisfying both

(i) $(u_1, \dots, u_n) \equiv (u_{i,1}, \dots, u_{i,n}) (\mathrm{mod} p_i^m)$ for every $i = 1, \dots, r$, and

(ii) $f(u_1, \dots, u_n) = 0$.

Nota bene. Suppose $(v_1, \dots, v_n)$ is a sequence of integers such that $f(v_1, \dots, v_n) = 0$ and such that for every $i = 1, \dots, r$ there exists an integer c_i with $c_i \not\equiv 0 \pmod{p_i}$ and with $(v_1, \dots, v_n) \equiv (c_i u_{i,1}, \dots, c_i u_{i,n}) (\mathrm{mod} p_i^m)$, then by the Chinese Remainder Theorem there exists an integer c such that for every $i = 1, \dots, r$, $cc_i \equiv 1 \pmod{p_i^e}$. And then for every $i = 1, \dots, r$, we have$(cv_1, \dots, cv_n) \equiv (u_{i,1}, \dots, u_{i,n}) \pmod{p_i^e}$. Since $f(cv_1, \dots, cv_n)$ equals $c^d f(v_1, \dots, v_n) = c^d \cdot 0 = 0$, then $(u_1, \dots, u_n) := (cv_1, \dots, cv_n)$ satisfies (i) and (ii). In the earlier draft of the problem set, the condition (i) above was different; it was the condition on $(v_1, \dots, v_n)$. But because of this observation, it is equivalent to the (simpler) condition (i).

Stated more loosely, weak approximation says that every collection of nontrivial local solutions at p_1 through p_r is "approximated to arbitrary order" by nontrivial integer solutions, i.e., for every integer m and for each collection of local solutions at $p_1, \dots, p_r$, there exists an integer solution which is congruent to each local solution modulo p_i^m.

By the same method as in **Problem 2**, show that for $g(v_1, \dots, v_n) = f(T(u_1, \dots, u_n))$, g satisfies weak approximation if and only if f satisfies weak approximation.

(5) Consider the integer, ternary quadratic form

$$f(x_1, x_2, x_3) = x_2^2 - x_1 x_3.$$

(5.a) Prove that every primitive integer solution of f is of the form $(u_1, u_2, u_3) = \pm(s^2, st, t^2)$ for relatively prime integers s and t. Conclude that every nontrivial integer solution is of the form $c(s^2, st, t^2)$ for a nonzero integer c and for relatively prime integers s and t.

(5.b) Let p be a prime integer. Let (u_1, u_2, u_3) be integers such that

(i) $(u_1, u_2, u_3) \not\equiv (0, 0, 0) \pmod{p}$, and

(ii) $f(u_1, u_2, u_3) \equiv 0 \pmod{p^m}$.

Prove that $(u_1, u_3) \not\equiv (0, 0) \pmod{p}$. Use this to prove that there exist integers c, s and t such that $c \not\equiv 0 \pmod{p}$ and $(u_1, u_2, u_3) \equiv c(s^2, st, t^2) \pmod{p^m}$.

Hint. Choose c to be either u_1 or u_3.

(5.c) Combine **(a)** and **(b)** with the Chinese Remainder Theorem to conclude that f satisfies weak approximation.

(6) Let $f(x_1, x_2, x_3)$ be a integer, ternary quadratic form which is in "Legendre diagonal form", i.e.,

$$f(x_1, x_2, x_3) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2,$$

for nonzero integers a_1, a_2, a_3 such that $a_1a_2a_3$ is a square-free integer. Let (u_1, u_2, u_3) be a primitive, integer solution of f.

(a) Show that the following 3×3 matrix T with integer entries has nontrivial determinant $D = -4a_1a_2a_3u_1^3$. And then prove that there exists a 3×3 matrix S with integer entries such that $TS = ST = D \cdot \mathbf{Id}_{3\times 3}$.

$$T = \begin{bmatrix} u_1a_2 & 0 & u_1a_3 \\ -u_2a_2 & -2u_3a_3 & u_2a_3 \\ u_3a_2 & -2u_2a_2 & -u_3a_3 \end{bmatrix}.$$

(b) Show that for the change of variables $(x_1, x_2, x_3)^\dagger = T(y_1, y_2, y_3)^\dagger$, the polynomial $g(y_1, y_2, y_3) = f(x_1, x_2, x_3) = f(T(y_1, y_2, y_3))$ equals

$$g(y_1, y_2, y_3) = D(y_2^2 - y_1y_3).$$

Combine this with **Problem 4** and **Problem 5** to conclude that $f(x_1, x_2, x_3)$ satisfies weak approximation.

(c) Again using **Problem 4**, show that for an integer, ternary quadratic form $h(z_1, z_2, z_3)$ which has a linear change of basis to a "Legendre diagonal form" $f(x_1, x_2, x_3)$ (which is always true if $\det(Q)$ is nonzero for the coefficient matrix Q of h), then h satisfies weak approximation assuming it has nontrivial real solutions and nontrivial local solutions at p for every prime p.