HMMT February 2015

Saturday 21 February 2015

Algebra

1. Let Q be a polynomial

$$Q(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

where $a_0, \ldots, a_n$ are nonnegative integers. Given that $Q(1) = 4$ and $Q(5) = 152$, find $Q(6)$.

Answer: $\boxed{254}$ Since each a_i is a nonnegative integer, $152 = Q(5) \equiv a_0 \pmod 5$ and $Q(1) = 4 \implies a_i \leq 4$ for each i. Thus, $a_0 = 2$. Also, since $5^4 > 152 = Q(5)$, $a_4, a_5, \ldots, a_n = 0$.

Now we simply need to solve the system of equations

$$5a_1 + 5^2 a_2^2 + 5^3 a_3^3 = 150$$
$$a_1 + a_2 + a_3 = 2$$

to get

$$a_2 + 6a_3 = 7.$$

Since a_2 and a_3 are nonnegative integers, $a_2 = 1$, $a_3 = 1$, and $a_1 = 0$. Therefore, $Q(6) = 6^3 + 6^2 + 2 = 254$.

2. The fraction $\frac{1}{2015}$ has a unique "(restricted) partial fraction decomposition" of the form

$$\frac{1}{2015} = \frac{a}{5} + \frac{b}{13} + \frac{c}{31},$$

where a, b, c are integers with $0 \leq a < 5$ and $0 \leq b < 13$. Find $a + b$.

Answer: $\boxed{14}$ This is equivalent to $1 = 13 \cdot 31a + 5 \cdot 31b + 5 \cdot 13c$.[1] Taking modulo 5 gives $1 \equiv 3 \cdot 1a \pmod 5$, so $a \equiv 2 \pmod 5$. Taking modulo 13 gives $1 \equiv 5 \cdot 5b = 25b \equiv -b \pmod{13}$, so $b \equiv 12 \pmod{13}$. The size constraints on a, b give $a = 2$, $b = 12$, so $a + b = 14$.

Remark. This problem illustrates the analogy between polynomials and integers, with prime powers (here $5^1, 13^1, 31^1$) taking the role of powers of irreducible polynomials (such as $(x-1)^1$ or $(x^2+1)^3$, when working with polynomials over the real numbers).

Remark. The "partial fraction decomposition" needs to be restricted since it's only unique "modulo 1". Abstractly, the abelian group (or $\mathbb{Z}$-module) $\mathbb{Q}/\mathbb{Z}$ has a "prime power direct sum decomposition" (more or less equivalent to Bezout's identity, or the Chinese remainder theorem), but $\mathbb{Q}$ itself (as an abelian group under addition) does not.

You may wonder whether there's a similar "prime power decomposition" of $\mathbb{Q}$ that accounts not just for addition, but also for multiplication (i.e. the full ring structure of the rationals). In some sense, the "adeles/ideles" serve this purpose, but it's not as clean as the partial fraction decomposition (for additive structure alone)—in fact, the subtlety of adeles/ideles reflects much of the difficulty in number theory!

3. Let p be a real number and $c \neq 0$ an integer such that

$$c - 0.1 < x^p \left(\frac{1 - (1+x)^{10}}{1 + (1+x)^{10}} \right) < c + 0.1$$

for all (positive) real numbers x with $0 < x < 10^{-100}$. (The exact value 10^{-100} is not important. You could replace it with any "sufficiently small number".)

Find the ordered pair (p, c).

[1] Note that this does actually have integer solutions by Bezout's identity, as $\gcd(13 \cdot 31, 5 \cdot 31, 5 \cdot 13) = 1$.

Answer: $\boxed{(-1,-5)}$ This is essentially a problem about limits, but phrased concretely in terms of "small numbers" (like 0.1 and 10^{-100}).

We are essentially studying the rational function $f(x) := \frac{1-(1+x)^{10}}{1+(1+x)^{10}} = \frac{-10x+O(x^2)}{2+O(x)}$, where the "big-O" notation simply make precise the notion of "error terms".[2]

Intuitively, $f(x) \approx \frac{-10x}{2} = -5x$ for "small nonzero x". (We could easily make this more precise if we wanted to, by specifying the error terms more carefully, but it's not so important.) So $g(x) := x^p f(x) \approx -5x^{p+1}$ for "small nonzero x".

- If $p+1>0$, g will approach 0 ("get very small") as x approaches 0 (often denoted $x \to 0$), so there's no way it can stay above the lower bound $c-0.1$ for all small nonzero x.
- If $p+1<0$, g will approach $-\infty$ ("get very large in the negative direction") as $x \to 0$, so there's no way it can stay below the upper bound $c+0.1$ for all small nonzero x.
- If $p+1=0$, $g \approx -5$ becomes approximately constant as $x \to 0$. Since c is an **integer**, we must have $c=-5$ (as -5 is the only integer within 0.1 of -5).

Remark. Why does $(p,c)=(-1,-5)$ actually satisfy the inequality? This is where the 10^{-100} kicks in: for such small values of x, the "error" $|g(x)-(-5)|$ of the approximation $g \approx -5$ does actually lie within the permitted threshold of ± 0.1. (You can easily work out the details yourself, if you're interested. It's something you might want to work out once or twice in your life, but rational functions are "well-behaved" enough that we can usually rely on our intuition in these kinds of scenarios.)

4. Compute the number of sequences of integers $(a_1,\dots,a_{200})$ such that the following conditions hold.

   - $0 \le a_1 < a_2 < \cdots < a_{200} \le 202$.
   - There exists a positive integer N with the following property: for every index $i \in \{1,\dots,200\}$ there exists an index $j \in \{1,\dots,200\}$ such that $a_i + a_j - N$ is divisible by 203.

   Answer: $\boxed{20503}$ Let $m := 203$ be an integer not divisible by 3. We'll show the answer for general such m is $m\lceil \frac{m-1}{2} \rceil$.

   Let x,y,z be the three excluded residues. Then N works if and only if $\{x,y,z\} \equiv \{N-x,N-y,N-z\} \pmod m$. Since $x,y,z \pmod m$ has opposite orientation as $N-x,N-y,N-z \pmod m$, this is equivalent to x,y,z forming an arithmetic progression (in some order) modulo m centered at one of x,y,z (or algebraically, one of $N \equiv 2x \equiv y+z$, $N \equiv 2y \equiv z+x$, $N \equiv 2z \equiv x+y$ holds, respectively).

   Since $3 \nmid m$, it's impossible for more than one of these congruences to hold (or else x,y,z would have to be equally spaced modulo m, i.e. $x-y \equiv y-z \equiv z-x$). So the number of distinct 3-sets corresponding to arithmetic progressions is $m\lceil \frac{m-1}{2} \rceil$ (choose a center and a difference, noting that $\pm d$ give the same arithmetic progression). Since our specific $m=203$ is odd this gives $m\frac{m-1}{2} = 203 \cdot 101 = 20503$.

   Remark. This problem is a discrete analog of certain so-called Frieze patterns. (See also Chapter 6, Exercise 5.8 of Artin's *Algebra* textbook.)

5. Let a,b,c be positive real numbers such that $a+b+c=10$ and $ab+bc+ca=25$. Let $m=\min\{ab,bc,ca\}$. Find the largest possible value of m.

   Answer: $\boxed{\frac{25}{9}}$ Without loss of generality, we assume that $c \ge b \ge a$. We see that $3c \ge a+b+c=10$. Therefore, $c \ge \frac{10}{3}$.

[2]For instance, the $O(x^2)$ refers to a function bounded by $C|x|^2$ for some positive constant C, whenever x is close enough to 0 (and as the 10^{-100} suggests, that's all we care about).

Since

$$\begin{aligned} 0 &\le (a-b)^2 \\ &= (a+b)^2 - 4ab \\ &= (10-c)^2 - 4\left(25 - c(a+b)\right) \\ &= (10-c)^2 - 4\left(25 - c(10-c)\right) \\ &= c(20-3c), \end{aligned}$$

we obtain $c \le \frac{20}{3}$. Consider $m = \min\{ab, bc, ca\} = ab$, as $bc \ge ca \ge ab$. We compute $ab = 25 - c(a+b) = 25 - c(10-c) = (c-5)^2$. Since $\frac{10}{3} \le c \le \frac{20}{3}$, we get that $ab \le \frac{25}{9}$. Therefore, $m \le \frac{25}{9}$ in all cases and the equality can be obtained when $(a,b,c) = (\frac{5}{3}, \frac{5}{3}, \frac{20}{3})$.

6. Let a, b, c, d, e be nonnegative integers such that $625a + 250b + 100c + 40d + 16e = 15^3$. What is the maximum possible value of $a + b + c + d + e$?

   Answer: $\boxed{153}$ The intuition is that as much should be in e as possible. But divisibility obstructions like $16 \nmid 15^3$ are in our way. However, the way the coefficients $5^4 > 5^3 \cdot 2 > \cdots$ are set up, we can at least easily avoid having a, b, c, d too large (speifically, ≥ 2). This is formalized below.

   First, we observe that $(a_1, a_2, a_3, a_4, a_5) = (5, 1, 0, 0, 0)$ is a solution. Then given a solution, replacing (a_i, a_{i+1}) with $(a_i - 2, a_{i+1} + 5)$, where $1 \le i \le 4$, also yields a solution. Given a solution, it turns out all solutions can be achieved by some combination of these swaps (or inverses of these swaps).

   Thus, to optimize the sum, we want $(a, b, c, d) \in \{0, 1\}^4$, since in this situation, there would be no way to make swaps to increase the sum. So the sequence of swaps looks like $(5, 1, 0, 0, 0) \to (1, 11, 0, 0, 0) \to (1, 1, 25, 0, 0) \to (1, 1, 1, 60, 0) \to (1, 1, 1, 0, 150)$, yielding a sum of $1 + 1 + 1 + 0 + 150 = 153$.

   Why is this optimal? Suppose (a, b, c, d, e) maximizes $a + b + c + d + e$. Then $a, b, c, d \le 1$, or else we could use a replacement $(a_i, a_{i+1}) \to (a_i - 2, a_{i+1} + 5)$ to strictly increase the sum. But modulo 2 forces a odd, so $a = 1$. Subtracting off and continuing in this manner[3] shows that we must have $b = 1$, then $c = 1$, then $d = 0$, and finally $e = 150$.

   Remark. The answer is coincidentally obtained by dropping the exponent of 15^3 into the one's place.

7. Suppose (a_1, a_2, a_3, a_4) is a 4-term sequence of real numbers satisfying the following two conditions:

   - $a_3 = a_2 + a_1$ and $a_4 = a_3 + a_2$;
   - there exist real numbers a, b, c such that

     $$an^2 + bn + c = \cos(a_n)$$

     for all $n \in \{1, 2, 3, 4\}$.

   Compute the maximum possible value of

   $$\cos(a_1) - \cos(a_4)$$

   over all such sequences (a_1, a_2, a_3, a_4).

   Answer: $\boxed{-9 + 3\sqrt{13}}$ Let $f(n) = \cos a_n$ and $m = 1$. The second ("quadratic interpolation") condition on $f(m)$, $f(m+1)$, $f(m+2)$, $f(m+3)$ is equivalent to having a vanishing third finite difference

   $$f(m+3) - 3f(m+2) + 3f(m+1) - f(m) = 0.$$

[3] This is analogous to the "number theoretic" proof of the uniqueness of the base 2 expansion of a nonnegative integer.

This is equivalent to

$$\begin{aligned} f(m+3)-f(m) &= 3\left[f(m+2)-f(m+1)\right] \\ \iff \cos(a_{m+3})-\cos(a_m) &= 3\left(\cos(a_{m+2})-\cos(a_{m+1})\right) \\ &= -6\sin\left(\frac{a_{m+2}+a_{m+1}}{2}\right)\sin\left(\frac{a_{m+2}-a_{m+1}}{2}\right) \\ &= -6\sin\left(\frac{a_{m+3}}{2}\right)\sin\left(\frac{a_m}{2}\right). \end{aligned}$$

Set $x=\sin\left(\frac{a_{m+3}}{2}\right)$ and $y=\sin\left(\frac{a_m}{2}\right)$. Then the above rearranges to

$$(1-2x^2)-(1-2y^2)=-6xy \iff x^2-y^2=3xy.$$

Solving gives $y=x\frac{-3\pm\sqrt{13}}{2}$. The expression we are trying to maximize is $2(x^2-y^2)=6xy$, so we want x, y to have the same sign; thus $y=x\frac{-3+\sqrt{13}}{2}$.

Then $|y|\le|x|$, so since $|x|,|y|\le 1$, to maximize $6xy$ we can simply set $x=1$, for a maximal value of $6\cdot\frac{-3+\sqrt{13}}{2}=-9+3\sqrt{13}$.

8. Find the number of ordered pairs of integers $(a,b)\in\{1,2,\dots,35\}^2$ (not necessarily distinct) such that $ax+b$ is a "quadratic residue modulo x^2+1 and 35", i.e. there exists a polynomial $f(x)$ with integer coefficients such that either of the following **equivalent** conditions holds:

   - there exist polynomials P,Q with integer coefficients such that $f(x)^2-(ax+b)=(x^2+1)P(x)+35Q(x)$;
   - or more conceptually, the remainder when (the polynomial) $f(x)^2-(ax+b)$ is divided by (the polynomial) x^2+1 is a polynomial with (integer) coefficients all divisible by 35.

   Answer: $\boxed{225}$ By the Chinese remainder theorem, we want the product of the answers modulo 5 and modulo 7 (i.e. when 35 is replaced by 5 and 7, respectively).

   First we do the **modulo 7 case**. Since x^2+1 is irreducible modulo 7 (or more conceptually, in $\mathbb{F}_7[x]$), exactly half of the nonzero residues modulo x^2+1 and 7 (or just modulo $x^2+\overline{1}$ if we're working in $\mathbb{F}_7[x]$) are quadratic residues, i.e. our answer is $1+\frac{7^2-1}{2}=25$ (where we add back one for the zero polynomial).

   Now we do the **modulo 5 case**. Since x^2+1 factors as $(x+2)(x-2)$ modulo 5 (or more conceptually, in $\mathbb{F}_5[x]$), by the **polynomial** Chinese remainder theorem modulo $x^2+\overline{1}$ (working in $\mathbb{F}_5[x]$), we want the product of the number of **polynomial** quadratic residues modulo $x\pm\overline{2}$. By centering/evaluating polynomials at $\mp\overline{2}$ accordingly, the polynomial squares modulo these linear polynomials are just those reducing to **integer** squares modulo 5.[4] So we have an answer of $(1+\frac{5-1}{2})^2=9$ in this case.

   Our final answer is thus $25\cdot 9=225$.

   Remark. This problem illustrates the analogy between integers and polynomials (specifically here, polynomials over the *finite field* of integers modulo 5 or 7), with $x^2+1 \pmod 7$ or $x\pm 2 \pmod 5$ taking the role of a prime number. Indeed, just as in the integer case, we expect exactly **half** of the (coprime) residues to be (coprime, esp. nonzero) quadratic residues.

9. Let $N=30^{2015}$. Find the number of ordered 4-tuples of integers $(A,B,C,D)\in\{1,2,\dots,N\}^4$ (not necessarily distinct) such that for every integer n, $An^3+Bn^2+2Cn+D$ is divisible by N.

   Answer: $\boxed{24}$ Note that $n^0=\binom{n}{0}$, $n^1=\binom{n}{1}$, $n^2=2\binom{n}{2}+\binom{n}{1}$, $n^3=6\binom{n}{3}+6\binom{n}{2}+\binom{n}{1}$ (generally see `http://en.wikipedia.org/wiki/Stirling_numbers_of_the_second_kind`). Thus the polynomial rewrites as

$$6A\binom{n}{3}+(6A+2B)\binom{n}{2}+(A+B+2C)\binom{n}{1}+D\binom{n}{0},$$

[4] This is more explicit than necessary. By the same reasoning as in the previous paragraph, we can abstractly count $1+\frac{5^1-1}{2}$ quadratic residues modulo $x\pm\overline{2}$ (irreducible polynomials in $\mathbb{F}_5[x]$) each (and then multiply/square to get the answer for $x^2+\overline{1}$).

which by the classification of integer-valued polynomials is divisible by N always if and only if $6A, 6A+2B, A+B+2C, D$ are always divisible by N.

We can eliminate B and (trivially) D from the system: it's equivalent to the system $6A \equiv 0 \pmod{N}$, $4A-4C \equiv 0 \pmod{N}$, $B \equiv -A-2C \pmod{N}$, $D \equiv 0 \pmod{N}$. So we want 1^2 times the number of (A, C) with $A \equiv 0 \pmod{N/6}$, $C \equiv A \pmod{N/4}$. So there are $N/(N/6) = 6$ choices for A, and then given such a choice of A there are $N/(N/4) = 4$ choices for C. So we have $6 \cdot 4 \cdot 1^2 = 24$ solutions total.

10. Find all ordered 4-tuples of integers (a, b, c, d) (not necessarily distinct) satisfying the following system of equations:

$$\begin{aligned} a^2 - b^2 - c^2 - d^2 &= c - b - 2 \\ 2ab &= a - d - 32 \\ 2ac &= 28 - a - d \\ 2ad &= b + c + 31. \end{aligned}$$

Answer: $\boxed{(5, -3, 2, 3)}$ We first give two systematic solutions using standard manipulations and divisibility conditions (with some casework), and then a third solution using quaternionic number theory (not very practical, so mostly for your cultural benefit).

Solution 1. Subtract the second equation from the third to get $a(c-b+1) = 30$. Add the second and third to get $2a(b+c) = -4-2d$. Substitute into the fourth to get

$$2a(2ad-31) = -4-2d \iff a(31-2ad) = 2+d \iff d = \frac{31a-2}{2a^2+1},$$

which in particular gives $a \not\equiv 1 \pmod{3}$. Then plugging in a factor of 30 for a gives us the system of equations $b+c = 2ad-31$ and $c-b+1 = 30/a$ in b, c. Here, observe that $b+c$ is odd, so $c-b+1$ is even. Thus a must be odd (and from earlier $a \not\equiv 1 \pmod{3}$), so $a \in \{-1, \pm 3, 5, \pm 15\}$. Manually checking these, we see that the only possibilities we need to check are $(a, d) = (5, 3), (-1, -11), (-3, -5)$, corresponding to $(b, c) = (-3, 2), (11, -20), (5, -6)$. Then check the three candidates against first condition $a^2 - b^2 - c^2 - d^2 = c - b - 2$ to find our only solution $(a, b, c, d) = (5, -3, 2, 3)$.

Solution 2. Here's an alternative casework solution. From $2ad = b+c+31$, we have that $b+c$ is odd. So, b and c has different parity. Thus, $b^2 + c^2 \equiv 1 \pmod{4}$. Plugging this into the first equation, we get that a and d also have the same parity.

So, $a^2 - b^2 - c^2 - d^2 \equiv -1 \pmod{4}$. Thus, $c - b - 2 \equiv -1 \pmod{4}$. So, $c \equiv b + 1 \pmod{4}$.

From taking modulo a in the second and third equation, we have $a \mid d + 32$ and $a \mid 28 - d$. So, $a \mid 60$.

Now, if a is even, let $a = 2k$ and $d = 2m$. Plugging this in the second and third equation, we get $2kc = 14 - k - m$ and $2kb = k - m - 16$. So, $k(c-b) = 15 - k$.

We can see that $k \neq 0$. Therefore, $c - b = \frac{15-k}{k} = \frac{15}{k} - 1$.

But $c - b \equiv 1 \pmod{4}$. So, $\frac{15}{k} - 1 \equiv 1 \pmod{4}$, or $\frac{15}{k} \equiv 2 \pmod{4}$ which leads to a contradiction.

So, a is odd. And we have $a \mid 60$. So, $a \mid 15$. This gives us 8 easy possibilities to check...

Solution 3. The left hand sides clue us in to the fact that this problem is secretly about quaternions. Indeed, we see that letting $z = a + bi + cj + dk$ gives

$$(z - i + j)z = -2 - 32i + 28j + 31k.$$

Taking norms gives $N(z-i+j)N(z) = 2^2 + 32^2 + 28^2 + 31^2 = 2773 = 47 \cdot 59$. By the triangle inequality, $N(z), N(z-i+j)$ aren't too far apart, so they must be $47, 59$ (in some order).

Thus $z, z-i+j$ are Hurwitz primes.[5] We rely on the following foundational lemma in quaternion number theory:

[5] For the purposes of quaternion number theory, it's simpler to work in the the Hurwitz quaternions $\mathbb{H} = \langle i, j, k, \frac{1+i+j+k}{2} \rangle_{\mathbb{Z}}$, which has a left- (or right-) division algorithm, left- (resp. right-) Euclidean algorithm, is a left- (resp. right-) principal ideal domain, etc. There's no corresponding division algorithms when we're working with the Lipschitz quaternions, i.e. those with integer coordinates.

Lemma. Let $p \in \mathbb{Z}$ be an integer prime, and A a Hurwitz quaternion. If $p \mid N(A)$, then the $\mathbb{H}A + \mathbb{H}p$ (a left ideal, hence principal) has all element norms divisible by p, hence is nontrivial. (So it's either $\mathbb{H}p$ or of the form $\mathbb{H}P$ for some Hurwitz prime P.)

In our case, it will suffice to apply the lemma for $A = -2-32i+28j+31k$ at primes $p = 47$ and $q = 59$ to get factorizations (unique up to suitable left/right unit multiplication) $A = QP$ and $A = P'Q'$ (respectively), with P, P' Hurwitz primes of norm p, and Q, Q' Hurwitz primes of norm q. Indeed, these factorizations come from $\mathbb{H}A + \mathbb{H}p = \mathbb{H}P$ and $\mathbb{H}A + \mathbb{H}q = \mathbb{H}Q'$.

We compute by the Euclidean algorithm:

$$\begin{aligned}
\mathbb{H}A + \mathbb{H}(47) &= \mathbb{H}(-2-32i+28j+31k) + \mathbb{H}(47) \\
&= \mathbb{H}(-2+15i-19j-16k) + \mathbb{H}(47) \\
&= [\mathbb{H}(47\cdot 18) + \mathbb{H}(47)(-2-15i+19j+16k)]\frac{-2+15i-19j-16k}{47\cdot 18} \\
&= [\mathbb{H}18 + \mathbb{H}(-2+3i+j-2k)]\frac{-2+15i-19j-16k}{18} \\
&= \mathbb{H}(-2+3i+j-2k)\frac{-2+15i-19j-16k}{18} \\
&= \mathbb{H}\frac{-54-90i+54j-36k}{18} \\
&= \mathbb{H}(-3-5i+3j-2k).
\end{aligned}$$

Thus[6] there's a unit[7] ϵ such that $P = \epsilon(-3-5i+3j-2k)$.

Similarly, to get P', we compute

$$\begin{aligned}
A\mathbb{H} + 47\mathbb{H} &= (-2-32i+28j+31k)\mathbb{H} + 47\mathbb{H} \\
&= (-2+15i-19j-16k)\mathbb{H} + 47\mathbb{H} \\
&= \frac{-2+15i-19j-16k}{47\cdot 18}[(47\cdot 18)\mathbb{H} + 47(-2-15i+19j+16k)\mathbb{H}] \\
&= \frac{-2+15i-19j-16k}{18}[18\mathbb{H} + (-2+3i+j-2k)\mathbb{H}] \\
&= \frac{-2+15i-19j-16k}{18}(-2+3i+j-2k)\mathbb{H} \\
&= \frac{-54+18i+18j+108k}{18}\mathbb{H} \\
&= (-3+i+j+6k)\mathbb{H},
\end{aligned}$$

so there's a unit ϵ' with $P' = (-3+i+j+6k)\epsilon'$.

Finally, we have either $z = \epsilon(-3-5i+3j-2k)$ for some ϵ, or $z - i + j = (-3+i+j+6k)\epsilon'$ for some ϵ'. Checking the $24+24$ cases (many of which don't have integer coefficients, and can be ruled out immediately) gives $z = iP = 5-3i+2j+3k$ as the only possibility.

Remark. We have presented the most conceptual proof possible. It's also possible to directly compute based on the norms only, and do some casework. For example, since $47 \equiv 3 \pmod 4$, it's easy to check the only ways to write it as a sum of four squares are $(\pm5)^2 + (\pm3)^2 + (\pm3)^2 + (\pm2)^2$ and $(\pm3)^2 + (\pm1)^2 + (\pm1)^2 + (\pm6)^2$.

Remark. For a systematic treatment of quaternions (including the number theory used above), one good resource is *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry* by John H. Conway and Derek A. Smith. A more focused treatment is the expository paper *Factorization of Hurwitz Quaternions* by Boyd Coan and Cherng-tiao Perng.

For an example of interesting research in this rather exotic area, see the *Metacommutation of Hurwitz primes* paper by Henry Cohn and Abhinav Kumar.

[6] Hidden computations: we've used $47\cdot 18 = 846 = 2^2+15^2+19^2+16^2$, and $18 = N(-2+3i+j-2k)$.

[7] i.e. one of $\pm1, \pm i, \pm j, \pm k, \frac{\pm1\pm i\pm j\pm k}{2}$