Generalizing and Implementing
Michael Hirschhorn's AMAZING Algorithm for Proving Ramanujan-Type Congruences

Edinah GNANG and Doron ZEILBERGER

Preamble

Let $p(n)$ be the number of integer partitions of n. Euler famously proved that

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{i=1}^{\infty} \frac{1}{1-q^i} \quad .$$

Srinivasa Ramanujan famously discovered (by glancing at a table of $p(n)$ for $1 \leq n \leq 200$, computed by the *analytic machine*, Major Percy Alexander MacMahon's head) the three congruences

$$p(5m+4) \equiv 0 \pmod 5 \quad ,$$

$$p(7m+5) \equiv 0 \pmod 7 \quad ,$$

$$p(11m+6) \equiv 0 \pmod{11} \quad .$$

The first two are really easy, and the proofs that G.H. Hardy chose to present in his classic book "Ramanujan" ([Ha], pp. 87-88), slightly streamlined, go as follows.

First recall the (purely elementary and *shaloshable*) identities of Euler and Jacobi :

$$E(q) = \prod_{i=1}^{\infty}(1-q^i) = \sum_{n=-\infty}^{\infty} (-1)^n q^{(3n^2+n)/2} \quad , \quad \textit{and}$$

$$E(q)^3 = \sum_{n=0}^{\infty}(-1)^n(2n+1)q^{(n^2+n)/2} \quad .$$

Also recall the obvious fact (but *extremely useful* [e.g. the AKS algorithm!]), that follows from the binomial theorem, that for every prime p, and any polynomial, or formal power series, $f(q)$, $f(q)^p \equiv f(q^p) \pmod p$. In particular $E(q)^p \equiv E(q^p) \pmod p$.

p(5n+4) is divisible by 5

Since $\{(n^2+n)/2 \; mod \; 5 \; ; \; 0 \leq n \leq 4 \; , \; 2n+1 \not\equiv 0 \pmod 5\} = \{0,1\}$, we have:

$$E(q)^3 = J_0 + J_1 \quad ,$$

where J_i consists of those terms in which the power of q is congruent to i modulo 5. Now

$$\sum_{n=0}^{\infty} p(n)q^n = E(q)^{-1} = \frac{(E(q)^3)^3}{E(q)^{10}} = \frac{(E(q)^3)^3}{(E(q)^5)^2} \equiv \frac{(J_0+J_1)^3}{E(q^5)^2} \pmod 5 \quad ,$$

and only powers congruent to $0, 1, 2, 3$ modulo 5 show up, and hence the coefficient of q^{5n+4} is always 0 modulo 5.

p(7n+4) is divisible by 7

Since $\{(n^2+n)/2 \; mod \; 7 \; ; \; 0 \le n \le 6 \; , \; 2n+1 \not\equiv 0 \pmod 7\} = \{0, 1, 3\}$, we have:

$$E(q)^3 = J_0 + J_1 + J_3 \quad ,$$

where J_i consists of those terms in which the power of q is congruent to i modulo 7. Now

$$\sum_{n=0}^{\infty} p(n) q^n = E(q)^{-1} = \frac{(E(q)^3)^2}{E(q)^7} \equiv \frac{(J_0 + J_1 + J_3)^2}{E(q^7)} \pmod 7 \quad ,$$

and none of the powers congruent to 5 modulo 7 show up, and hence the coefficient of q^{7n+5} is always 0 modulo 5.

At the bottom of page 88 of Hardy's above-mentioned classic "Ramanujan"[Ha], he states

"*There does not seem to be an equally simple proof that* $p(11n+6)$ *is divisible by* 11".

Over the years there were many proofs, but **none** as **simple** and **elementary** and, most importantly, **beautiful!** as the one recently found by Michael Hirschhorn [Hi].

Michael Hirschhorn's proof for p(11n+6)

The proof in [Hi] goes like this. It starts the same way:

$$E(q)^3 \equiv J_0 + J_1 + J_3 + J_6 + J_{10} \pmod{11} \quad ,$$

where J_i consists of those terms in which the power of q is congruent to i modulo 11. Now

$$\sum_{n=0}^{\infty} p(n) q^n = E(q)^{-1} = \frac{(E(q)^3)^7}{E(q)^{22}} \equiv \frac{(J_0 + J_1 + J_3 + J_6 + J_{10})^7}{E(q^{11})^2} \pmod{11} \quad .$$

Alas, now the part consisting of the powers that are congruent to 6 modulo 11 in the polynomial $(J_0 + J_1 + J_3 + J_6 + J_{10})^7 \pmod{11}$ is **not** identically zero modulo 11, but a certain polynomial of degree 7 in $\{J_0, J_1, J_3, J_6, J_{10}\}$, (over $GF(11)$) let's call it P.

But we also have

$$E(q) = E_0 + E_1 + E_2 + E_4 + E_5 + E_7$$

where E_i consists of those terms in which the power of q is congruent to i modulo 11, and

$$(E(q)^3)^4 = E(q)^{12} = E(q)^{11} E(q) \equiv E(q^{11}) E(q) \pmod{11} \quad ,$$

so

$$(J_0 + J_1 + J_3 + J_6 + J_{10})^4 \equiv E(q)^{12} \pmod{11} \equiv E(q^{11})(E_0 + E_1 + E_2 + E_4 + E_5 + E_7) \pmod{11} \quad .$$

By expanding the left side and extracting the complementary powers $\pmod{11}$ ($\{3,6,8,9,10\}$), we get five polynomials of degree 4, let's call them $P_3, P_6, P_8, P_9, P_{10}$. Then we ask our beloved computer to find five polynomials of degree 3, (in the variables $\{J_0, J_1, J_3, J_6, J_{10}\}$), let's call them $Q_3, Q_6, Q_8, Q_9, Q_{10}$, such that

$$P \equiv Q_3P_3 + Q_6P_6 + Q_8P_8 + Q_9P_9 + Q_{10}P_{10} \pmod{11} \quad .$$

Since it succeeded (*a priori* there was no guarantee!), we are done!! *Quod Erat Demonstratum.*

See the output file `http://www.math.rutgers.edu/~zeilberg/tokhniot/oHIRSCHHORN1v`, that contains the above three proofs, (and four other ones!), that was generated, by running `HIRSCHHORN`, in three seconds!

Generalization

Let's consider, more generally,

$$\sum_{n=0}^{\infty} p_{-a}(n)q^n = \prod_{i=1}^{\infty} \frac{1}{(1-q^i)^a} \quad .$$

(Note that $p_{-1}(n) = p(n)$ and $p_{24}(n) = \tau(n-1)$, where $\tau(n)$ is Ramanujan's τ-function).

Now let's do an exhaustive computer search for congruences of the form

$$p_{-a}(Pn + r) \equiv 0 \pmod{P} \quad ,$$

for primes $P \leq 101$, and $1 \leq a \leq 50$.

[[1, 4, 5], [1, 5, 7], [1, 6, 11], [2, 2, 5], [2, 3, 5], [2, 4, 5], [3, 7, 11],

[3, 15, 17], [5, 8, 11], [5, 5, 23], [7, 9, 19], [9, 17, 19], [9, 9, 23],

[21, 42, 47]]

By pure guessing, our beloved servant, Shalosh B. Ekhad, discovered the following 14 successful triples (rediscovering, for $a = 1$, the original three Ramanujan congruences).

$$[a, r, P] \in \{[[1,4,5],[1,5,7],[1,6,11],$$

[2, 2, 5], [2, 3, 5], [2, 4, 5]

[3, 7, 11], [3, 15, 17],

[5, 8, 11], [5, 5, 23],

$$[7,9,19],$$

$$[9,17,19],[9,9,23],$$

$$[21,42,47]\} \quad .$$

Silviu Radu [R2] kindly showed us how to deduce these (except for the last two, that we are sure can be done just as easily) from his powerful algorithm.

But it is still nice to have a *purely elementary* proof, in the style of Hirschhorn. This is implemented in the Maple package

`http://www.math.rutgers.edu/~zeilberg/tokhniot/HIRSCHHORN` .

For primes up to 11 it works in a few seconds, alas, a naive implementation of Hirschhorn's method, using "undetermined coefficients" runs ouf of memory.

Luckily we have *Gröbner Bases* and the *Buchberger* algorithm. The question boils down to proving that P belongs to the *radical* of the ideal generated by the P_i-s. Even here things run out of time and memory (in Maple), but since we are working over $GF(p)$, by getting sufficiently many specializations, it is possible to prove ideal memberships for many special cases. Then we can either do *all* possible p^r specializations of freezing (any) r of the variables $\{J[i]\}$, or a *semi-rigorous* proof if we do a small random selection.

Since Radu[R1] has his powerful algorithm, we didn't bother to finish this up, but we know that it is *possible* to always try to do it. Of course, it is possible, but unlikely, that some congruences are not provable by Hirschhorn's elementary approach. So let us conclude with a

Meta Conjecture: **Any** Ramanujan-type congruence for so-called modular forms, that Radu[R1] famously proved is always doable with his powerful algorithm, that uses the deep theory of modular forms and functions, can also be done by *only* using Hirschhorn's elementary approach as extended in this article, together with the purely elementary Buchberger algorithm over finite fields.

Readers are welcome to see the front of this article for sample input and output.

`http://www.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/hirschhorn.html` .

Acknowledgement: We are grateful to Lev Borisov for insightful advice, and to Silviu Radu for permission to post [R2] and for useful discussion.

References

[Ha] G.H. Hardy, *"Ramanujan"*, Cambridge University Press, 1940.

[Hi] Michael D. Hirschhorn, *A short and simple proof of Ramanujan's mod 11 partition congruence*, preprint available from
`http://web.maths.unsw.edu.au/~mikeh/webpapers/paper188.pdf`

[R1] Silviu Radu, *An algorithmic approach to Ramanujan's congruences*, Ramanujan J. **20** (2009), 215-251 .

[R2] Silviu Radu, *Email message to Doron Zeilberger*,
`http://www.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/SilviuRaduMessageJune2013.pdf`

Edinah K. Gnang, Computer Science Department, Rutgers University (New Brunswick), Piscataway, NJ 08854, USA. `gnang at cs dot rutgers dot edu`

Doron Zeilberger, Mathematics Department, Rutgers University (New Brunswick), Piscataway, NJ 08854, USA. `zeilberg at math dot rutgers dot edu`