Largest idempotent

Given the prime power factors of N, is there a non-quadratic algorithm for finding the **largest** idempotent of ring $\mathbb{Z}/N\mathbb{Z}$? (That is, the largest number $A < N$ such that $A^2 \equiv A \bmod N$.)

I know that there are at most 8 prime power factors ($= K$) for N in the range of interest, thus at most $256 (= 2^K)$ idempotents, with 0 & 1 being trivial.

edited: "range of interest" clause somehow got misplaced.

(number-theory) (algorithms)

edited Jan 9 '13 at 6:10
hardmath 20.4k 5 32 70

asked Jan 7 '13 at 21:41
Jerry B 21 2

1 By "ring N," do you mean $\mathbb{Z}/N\mathbb{Z}$? And in this case, by "largest," do you mean largest in the range $\{0, 1, \dots, N-1\}$? – Paul VanKoughnett Jan 7 '13 at 22:06

1 From the context, it looks like you are just interested in the ring $\mathbb{Z}/(N)$? – rschwieb Jan 7 '13 at 22:06

@Paul Yes, $\mathbb{Z}/n\mathbb{Z}$. I didn't know how to make the notation on here. And yes, the largest integer value. – Jerry B Jan 8 '13 at 3:25

So you want sub-quadratic in terms of N? Maybe order the prime power factors in terms of descending magnitude and then use CRT to find a number congruent to 1 to all but the smallest and congruent to 0 to that one. – JSchlather Jan 8 '13 at 3:38

@JacobSchlather Thank you, that was a very productive suggestion. Unfortunately, it turns out using 0 for the smallest factors doesn't guarantee the solution will be the largest idempotent. So, it looks like I'll have to calculate all 2^n-2 non-trivial idempotents and select the largest. – Jerry B Jan 8 '13 at 9:37

There is a symmetry that might(?) be useful in some sort of approach. Since $1-e$ is an idempotent whenever e is, finding very small idempotents yields very large idempotents. – rschwieb Jan 8 '13 at 13:50

@rschwieb I was aware of that, which may cut the 2^K numbers to test down to 2^{K-1}. Using the general solution of the CRT

$$\sum_i a_i \frac{N}{n_i}\left[\frac{N}{n_i}\right]^{-1}_{n_i}$$

calculated for each set of a_i taking the values 0 and 1 will find all 2^K idempotents. Is it the case that solving for a={0,1,1,1} and a={1,0,0,0} (inverting the 1's and 0's) will produce the 2 solutions that add to $N+1$? If so, that will cut my calculation in half. – Jerry B Jan 8 '13 at 23:58

Note that the CRT problems we're asked to solve are of a special form, $x \equiv 0 \mod M$ and $x \equiv 1 \mod (N/M)$ where factors M and N/M are coprime. The solution will be a multiple of M, so somewhat unintuitively a heuristic exists for making M as large as possible. – hardmath Jan 9 '13 at 3:29

I have reached an odd point. After checking my code repeatedly, and 2 variations that produced the same result, I broke down and googled it. Somehow, my solution is off by exactly 1. The basic algorithm had to be correct, or it wouldn't have gotten that close. I was totally at a loss as to where this extra 1 came from. And then I realized, N=1 was being treated as a prime, for M(1)=1. It should be M(1)=0. Always watch your edge cases! – Jerry B Jan 9 '13 at 7:55

1 Answer

Let $N = m_1 \dots m_k$ be a prime power decomposition (distinct m_i coprime).

Then A is an *idempotent* modulo N iff $A^2 \equiv A \mod N$. Equivalently, A is an idempotent modulo each prime power factor m_i, which amounts to:

$$\forall m_i \; A \equiv 0, 1 \mod m_i$$

because $A(A-1)$ is divisible by prime power m_i only if m_i divides A or $A-1$. Henceforth we will refer to $0, 1$ as *trivial* idempotents. For *nontrivial* idempotents A we multiply those factors m_i which divide A to get the product M. Then M and N/M are coprime and:

$$A \equiv 0 \mod M$$

$$A \equiv 1 \mod N/M$$

The first of these relations implies that $A = aM$. Require a reduced residue $1 < A < N$, and it follows $0 < a < N/M$. The coprimality of M and N/M gives $a \equiv M^{-1} \mod N/M$, thereby satisfying the second relation.

Moreover as @rschwieb pointed out, the nontrivial idempotents occur in pairs A, A' s.t. $A + A' = N + 1$ by swapping the roles of M and N/M. Searching for large idempotents (but less than N) thus amounts to searching for small ones (but greater than 1).

All nontrivial idempotents may be formed as distinct sums of "basic" idempotents A_i, $1 \leq i \leq k$, taking the product M_i of the $k-1$ prime powers *other* than m_i, so $N/M = m_i$. Then $A_i = a_i M_i$ where $a_i \equiv M_i^{-1} \mod m_i$. One way to solve for a_i uses the extended Euclidean algorithm to provide:

$$a_i M_i + b_i m_i = 1$$

Alternatively one can apply Euler's generalization of Fermat's Little Theorem:

$$a_i \equiv M_i^{\phi(m_i)-1} \mod m_i$$

However one computes those k basic solutions $a_i M_i$, all nontrivial idempotents $\mod N$ can be expressed as sums over proper (nonempty) subsets of them. By this accounting there are $2^k - 2$ of them (excludes the two trivial idempotents).

Example: Let $N = 10^n = 2^n 5^n$. For each n there are two nontrivial idempotents, adding up to $N+1$. Their respective decimal representations "stabilize" by truncation so we may summarize both parallel expansions:

$$a_n 5^n : \ \ldots 19977392256259918212890625$$

$$b_n 2^n : \ \ldots 80022607743740081787109376$$

allowing us to tell by inspection for given n which of the two is larger. I don't see any regular pattern in these results, although the frequency of double digits looks somewhat improbable.

Cases of this turn up in online puzzles and older literature.

Readers interested in extending this example may find it useful that squaring an initial segment of the $a_n 5^n$ adds at least one extra correct digit. The analogous fact about the $b_n 2^n$ series requires taking a fifth power, so it's more easily derived by "complementing" the $a_n 5^n$ series.

The irregularity with which the above two series of idempotents swap top position doesn't suggest a shortcut for more general N and higher number of factors k.

While an exhaustive search is satisfactory for small k, for large k we should perhaps look to the subset sum problem for inspiration.

The set of basic solutions $\{A_1, \ldots, A_k\}$ can without loss of generality be assumed to be ordered. So as a first approximation to finding the largest nontrivial idempotent, we can compare A_k and $N + 1 - A_1$. No single basic solution (or sum of $k-1$ of them) could improve on that, so let's label that E_1.

Using two or basic solutions for an improvement would then amount to a sequence of approximate subset sum problems targeting intervals $((j-1)N + E_j, jN - 1]$ for $j = 1$ up to $\frac{k}{2}$, taking E_{j+1} to be the improvement if one is found, or E_j otherwise.

While this seems promising as far as polynomial-time in k, it's only a sketch of an idea at this point.

answered Jan 12 '13 at 19:50

hardmath
20.4k 5 32 70

Thanks. In the end, trying to program your suggested optimization would take me longer to program than the "check $2^k - 2$ possibilities" already runs (about 1 hour). Fortunately, $k < 9$ for my problem, so it's not so bad. – Jerry B Jan 13 '13 at 4:37

@JerryB: Thanks for taking the time to move the Question here from StackOverflow. With many hard problems a theoretical improvement in complexity only has a practical benefit at very large scales, even discounting the months of additional development. However I suspect running time of exhaustive search should only be taking less than a minute for k=8. Would you care to post a value of N that illustrates the Question? – hardmath Jan 13 '13 at 13:53

Well, the 1 hour runtime is actually for **all** N values 1 thru 10^7. The maximum k=8 is for the integer with the largest number of prime power factors in that range. – Jerry B Jan 14 '13 at 0:25