# Disproving the Converse, of the concept, that a witness squared, equaling 1 in a modulus, disproves the modulus to be prime.

Dirk Mittler

Thursday, May 30, 2019

The exact equation may differ for small integers, but for large integers, such as $\left(n = 2^{256}\right)$, the probability of any one being a perfect square is approximately like so `http://dirkmittler.homeip.net/PPerf_Sq_1.pdf` :

$p_0 \approx \left(\frac{1}{2\sqrt{n}}\right)$

The probability we are more interested in however, is of every multiple $(0 < k \leq n)$ of a modulus $(n)$, plus (1), not being square, which will lead to the situation that $\left(a^2 mod\, n \neq 1\, \forall a\right)$. Through common-sense analysis, and ignoring the cases where $(a \in \{1, n-1\})$, this probability seems to correspond to the product series:

$p \approx \prod_{k=1}^{n} \left(1 - \frac{1}{2\sqrt{kn}}\right)$

In order to solve this product series, the approximations will be used that, for very small values of $(x)$:

$e^x \approx 1 + x,$
$x \approx \ln|1 + x|.$

Thus, the substitution can be made:

$x = \frac{1}{2}(kn)^{-\frac{1}{2}}$

Resulting in the summation series:

$\ln|p| \approx \sum_{k=1}^{n} -\frac{1}{2}(kn)^{-\frac{1}{2}},$

$\ln|p| \approx -\frac{1}{2}n^{-\frac{1}{2}} \sum_{k=1}^{n} k^{-\frac{1}{2}}.$

Finally, the summation can be simplified as an integral:

$\ln|p| \approx -\frac{1}{2}n^{-\frac{1}{2}} \left(\int_{k=1}^{n} k^{-\frac{1}{2}}\, dk\right),$

$\ln|p| \approx -\frac{1}{2}n^{-\frac{1}{2}} \left(2n^{+\frac{1}{2}} + C\right).$

And, if $(n)$ is very large, then $\left(-\frac{1}{2}C\, n^{-\frac{1}{2}}\right)$ will become very small and can be neglected, leaving us with:

$\ln|p| \approx -n^{-\frac{1}{2}}n^{+\frac{1}{2}} = -1.$

$\therefore p \approx e^{-1} \approx 0.36787944$

Afterthought:

In order to obtain slightly more-accurate results, the endpoints of the product series can be adjusted, and the integral could be maintained as a definite integral. For example, in order to account for the fact that $\left(1^2 mod\, n\right) = 1$, the possibility would need to be included that $(k = 0)$, which is included in the indefinite integral above. This certain result will also lead to a divide-by-zero in the series, and thus, to an apparently infinite probability. The divide-by-zero originates over the attempted use of my generalization, in order to determine the probability with which (0) is a perfect square. The logical answer to that can be decided independently of my generalization.

The situation can take place often, that Humans know a factual property of an element of a set, without this knowledge affecting the generalized equations, for the probability with which the same element of the set would hypothetically have that property. One way to formalize this situation is, to restate the probability, as the probability that elements 'in the vicinity of' that one element, have the property in question, not that the exact element has it.

Another, allegorical way to formalize this concept is, to state that a person in Society matches a description in a limited number of ways, for which reason such a person has a probability, of possessing certain properties. If the person needed to match a description 'in every way', then the result would be an alias for another person, and not a probability (of the person being considered, perhaps being different despite this exact matching).

Additionally, the fact could be acknowledged that the product:
$\left((n-1)^2 mod\, n = 1\right)$ should not be tested for, being too high as the upper endpoint, for which reason:
$((n-1)n \rightarrow (k = n-1))$ should also be too high as the upper endpoint, so that maximally,
$(k = n-2)$ would be considered, even though again, that might be considered too high an endpoint. But then the Mathematical simplicity of the solution would be compromised, even though the solution presented here can be adapted to the reality of both endpoints, and the quantitative results would be negligible, through the division by $\left(1 - \frac{1}{2n}\right)$ etc., or, through the addition of $\left(+n^{-\frac{1}{2}}\right)$ to the exponent of $(e)$. Division of the final result by $\left(1 - \frac{1}{2n}\right)$ twice, when $\left(\frac{1}{2n}\right)$ is very small, can be approximated using the same 'lemma' substitution as was used in the main exercise, as the addition of $\left(+n^{-1}\right)$ to the exponent of $(e)$. But then again, when $\left(n = 2^{256}\right)$, neither additional term in the exponent would remain stored, after an addition to $(-1)$, using regular, double-precision floating-point numbers.

And so while such adjustments may 'look nice' algebraically, they would not affect the basic result.

$(n-2)n + 1 \equiv (n-1)(n-1)$

-Dirk Mittler