素数，朴素的素

原创

不争之德 于 2020-07-09 13:39:23 发布 153 收藏
分类专栏： 数学补习班 文章标签： 算法 python

本文链接：https://blog.csdn.net/qq_35089484/article/details/107225910


数学补习班 专栏收录该内容
1 篇文章 0 订阅
订阅专栏

素数，朴素的素

这几个月，也算是心里膨胀到极点了，居然开始参加CTF了。而且都是参加好难好难的比赛，而且还是没有接受专业培训就参加比赛的。好在有一个队友，要不然自己都怕怕的。

每次参赛基本上就是只能做一下签到题，基本上也不用写什么writeup，因为签到题基本上就是玩游戏或者直接复制标准答案啦。不过虽然每次都做不出正题来，但是还是学到了很多东西，就比如Crypto的题目，RSA就是最常见的，每次比赛都至少有一道。

而我每次都会以为自己要做出来了，结果怎么算都没有结果。

学习用sagemath

每次参加CTF都会遇到一个RSA的题目，关于RSA的算法这里我就不贴了，反正大家都能找到，不过比赛里面用到的多半是变种。因为每次试着用Python的solve或者fsolve求解带有取余运算的方程都无果，无奈开始找更加高级的工具。听了一堂腾讯的公开课，主讲0ops战队的队长介绍了几个工具，其中就有sagemath，开源免费，嗯，适合我。

sagemath下载地址 https://www.sagemath.org/

我意外的发现sagemath在求解素数相关问题好像很擅长啊，而且计算速度好快。我在试着求解因子分解的时候决定用next_prime，previous_prime这些函数试根，居然秒秒钟就给出了一个素数。当然，我并没有试出来（T_T)

出于好奇，我就去看sagemath的源码，想知道为什么这些函数这么快。
源码地址在这里，https://github.com/sagemath/sage/tree/develop/src/sage/arith

（Github还不错，现在源码里可以navigate，点击一个函数的名称可以跳转到该函数的源码，大家自己找一下想要的函数，国内网速还是有些慢的，你们有条件就科学上网吧。）

然而看了源码以后备受打击，因为根本看不懂！虽然也是python写的，但是里面用到了ring这种数学概念，百度一下，什么高斯整数环之类的。关于这个整数环和sagemath的函数，我觉得有必要单开一篇来讲，等我研究清楚之后吧（：P）

素数给我们的启示

其实RSA里面用到了素数，素数的运算有很好的不可逆性，这些性质来源于素数一种很好的品质——一个素数，只能被自己和1整除。如果把除法当作一种解构的方式的话，素数其实很强大，它不能被解构。（我们暂时忽略被1整除的问题，被1整数其实就是证明自己是整数而已啦）

素数其实很不合群，因为除了1以外和其他数就没有公因子，换句话说就没有共同爱好啦，好可怕啊，这就是人世间所说的奇葩吧。不过有时候，静下心来想想，真的会有两个人的兴趣爱好完全相同吗？也许那只是一种错觉呢，也许我们就是认同与这种错觉呢，然后被各种认同分割得四分五裂。

所以，我没有把素数成为质数，因为我好喜欢这样的素数，朴素的素。如果一个数字真实面对自己，认同与自己目前的状况，而不去追逐外在的所谓认同，那么它就可以这么强大，那么一个人是不是也可以？

突然想到了一个人——拉马努金，那个印度的天才数学家，据说每一个整数都和他是好朋友，这个人一生都只对数学感兴趣，很不合群，但是他确实创造了近乎奇迹的数学创造，在历史的长河中为人类闪耀了一次。当然我们不是都需要变成他一样，况且我们也无法变成他一样，但是我们如果找到自己真正感兴趣的事物，专注的投入其中，也是很好的事情。做一个素数，你愿意吗？

有人说所有科学学到最后都是哲学，也许所有科学学到最后都是数学。哎，我怎么觉得之前的学都白上了呢，现在开始真正的学习吧。每天进步一点点，借CSDN的宝地做一些记录，希望有一天在回首往事的时候，能够告诉自己，时间没有虚度。