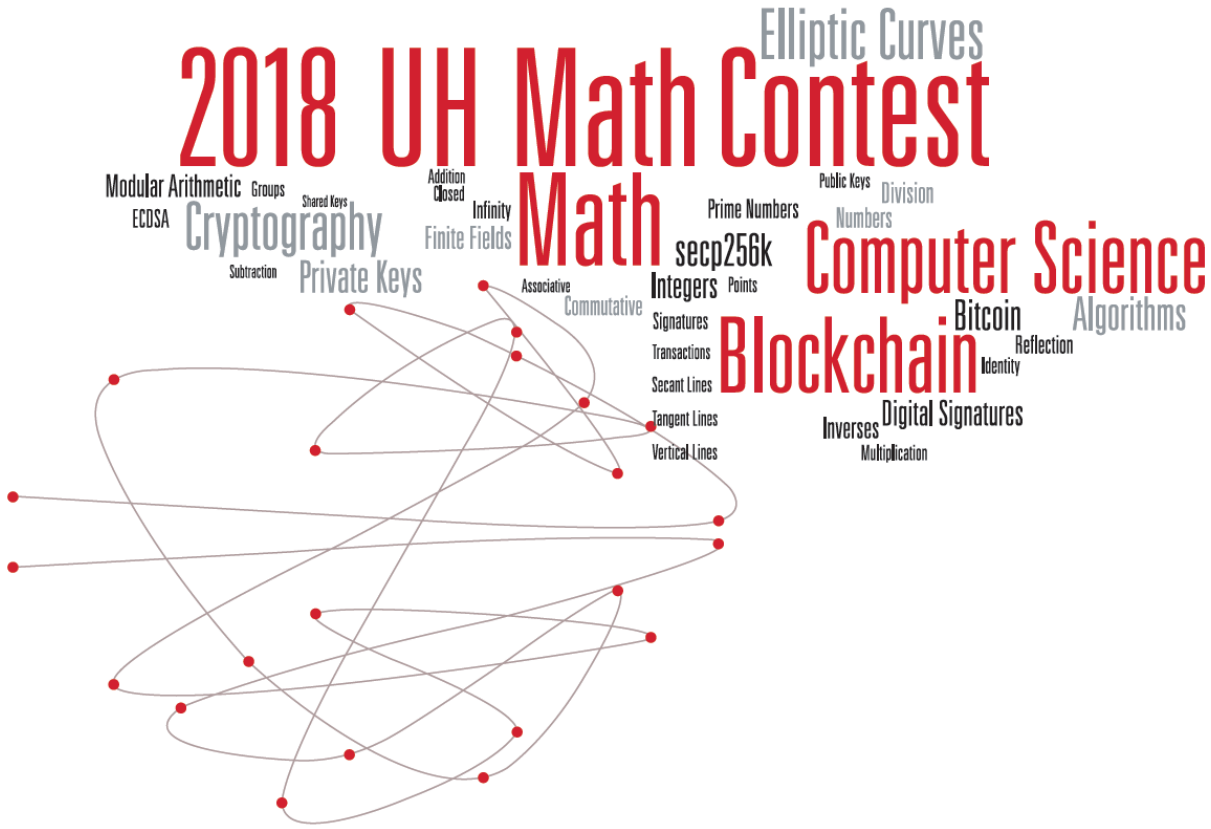
2018 Project Problem

University of Houston

An Introduction to the
Mathematics Behind Bitcoin and Blockchain



Cyclic subgroup of $y^2 = x^3 + 7 \bmod 23$
generated by (1,10), excluding the point at infinity

An Introduction to the Mathematics Behind Bitcoin and Blockchain

I feel confident that most of you have heard about the crypto currency Bitcoin, either through a news source or some form of social media. There has been a frenzy of activity associated with Bitcoin and other crypto currencies, and fortunes will be made and lost by investors. Regardless of whether Bitcoin is eventually adopted for wide use, the technology supporting Bitcoin, known as Blockchain, could prove to be even more valuable. This project encourages you to learn something about the mathematics associated with this technology.

Rules: Teams can consist of no more than 4 students who are zoned to the same school, or a feeder pair of schools (middle school and high school).

Directions: Assemble your team. Then type a report that introduces your team, details their contributions to the project, and gives an introduction to the mathematics behind Blockchain. Also, create an associated video presentation (no longer than 10 minutes) that gives a fun, informative introduction to the topic. Everyone on your team must play a nontrivial role in the video, and credits must appear at the end of the video, detailing the contribution of each team member.

Your typed report must include the definition of elliptic curves, give plots of various elliptic curves over R, define addition of points and the group law on elliptic curves over R, define the notion of the point at infinity, define F_p where p is a prime number, discuss F_p as a field (where p is a prime number), discuss the use of the extended Euclidean algorithm to find inverses of numbers and help perform division on F_p, give plots of various elliptic curves over F_p, and give a simple example showing how a digital signature can be verified using the ideas behind elliptic curve cryptography.

Words/phrases that must occur in your video: Elliptic Curves, Points, Groups, Closed, Associative, Commutative, Inverses, Identity, Vertical Lines, Tangent Lines, Secant Lines, Point at Infinity, Finite Field, Prime Numbers, Integers, Numbers, Addition, Subtraction, Multiplication, Division, Algorithms, Reflection, Modular Arithmetic, Blockchain, Cryptography, Math, Computer Science, secp256k1, Public Keys, Private Keys, Shared Keys, ECDSA, Digital Signatures, Transactions, Signatures and Bitcoin.

There are numerous documents and tutorials available online, with many of them containing all of this information. There are also many online plotting and computing devices associated with these ideas. Some examples include

http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/

https://www.coindesk.com/math-behind-bitcoin/

http://graui.de/code/elliptic2/

I know you will find many others, and benefit from the ideas in these sources. But I'll be looking for YOUR TEAM'S WORK.

Project solutions should be submitted by sending an email to drjeffmorgan@gmail.com by 9am on January 27th. Your email must include the name of the school, the name(s) of the team members, and links to your report and video. Do NOT send your report and video as attachments. For example, you can place your report on a Google Drive, and your video can be hosted on YouTube. In both cases, links can be created and placed in your email. There are a multitude of other options using similar online tools.

Please use the subject line 2018 TEAM PROJECT in your email submission.

You can email questions and comments, prior to your submission, to drjeffmorgan@gmail.com. As above, use the subject line 2018 TEAM PROJECT.

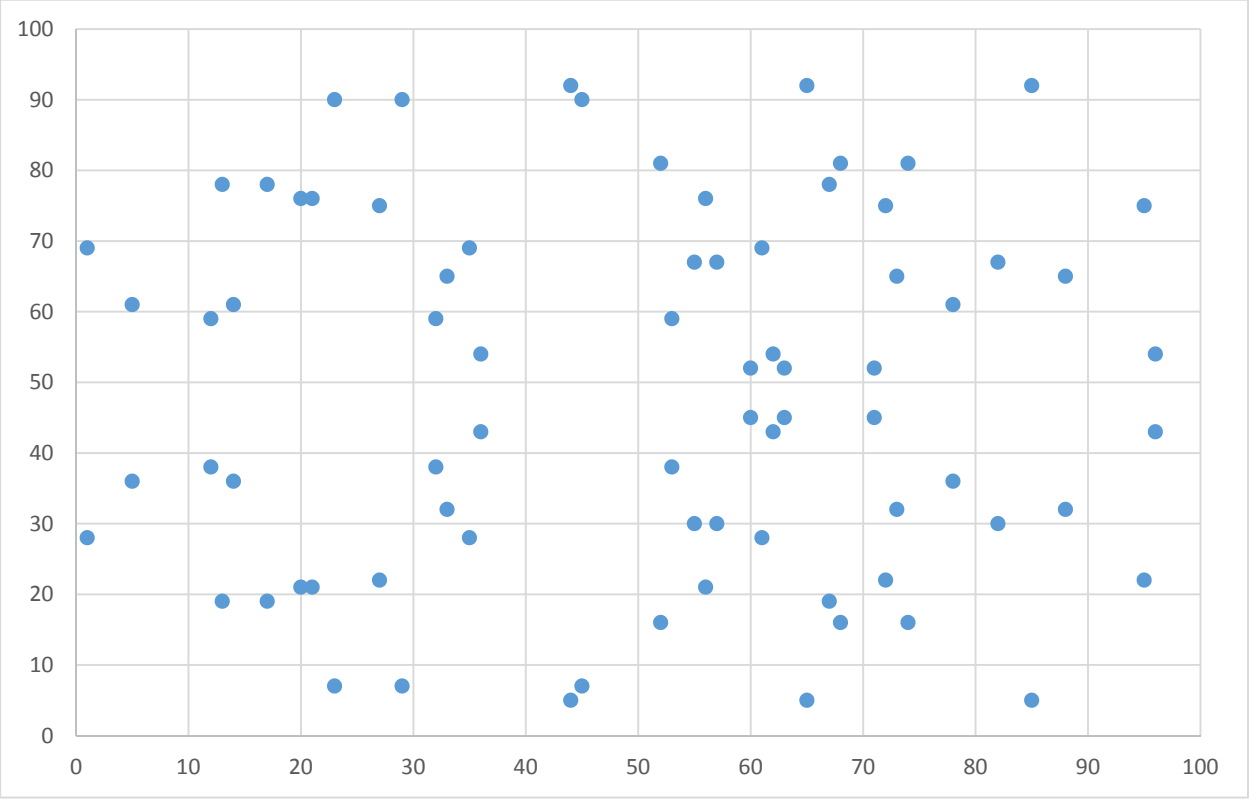
Project Evaluation:

Project submissions will be evaluated using the following criteria:

- Organization.
- Creativity.
- Clarity of presentation.
- Correctness.

Good luck! I look forward to reading your reports and watching your videos.

Dr. Jeff Morgan



$y^2 = x^3 + 7 \bmod 97$