

Last Bit of $F(x)$ Is Not So Random After All

Look more carefully...

46, 113, 92, 175, 42, 141, 152, 11, and so forth

Maybe the low bit isn't so random after all.

Remember: **$F(x) = (313x + 307) \bmod 256$**

- **Any even value of x gives odd $F(x)$**
- **and vice-versa.**